Department of the Army
Headquarters United States Forces Command
1777 Hardee Avenue, SW.
Fort McPherson, Georgia 30330-1062
1 August 1999

FORSCOM Regulation 190-13

Military Police
FORSCOM Physical Security Program

History. This is the first printing of FORSCOM Regulation 190-13.
Summary. This regulation establishes the FORSCOM Physical Security Program and provides MACOM guidance to DOD/HQDA physical security policy. The FORSCOM Physical Security Program is a component of the FORSCOM Force Protection Program.
Applicability. This regulation applies to all FORSCOM assigned and attached active and reserve Army units.
Supplementation. This regulation will not be supplemented without prior approval from HQ, FORSCOM ATTN: AFPM-FP, 1777 Hardee Avenue, SW., Fort McPherson, Georgia 30330-1062.
Changes. Changes to this regulation are not official unless authenticated by C/S, FORSCOM. Changes will be destroyed on their expiration dates unless sooner superseded or rescinded.
Suggested Improvements. The proponent of this regulation is Provost Marshal, HQ, FORSCOM (AFPM-FP), (404) 464-5909. Users may send comments and suggested improvements to this publication on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, FORSCOM, ATTN: AFPM-FP, 1777 Hardee Avenue, SW., Fort McPherson, Georgia 30330-1062, or via electronic mail (phy.sec.@forscom.army.mil).
Restrictions. This regulation is approved for public release with unlimited distribution. Local reproduction authorized.

FOR THE COMMANDER:

OFFICIAL:

JOHN M. PICKLER
Lieutenant General, USA
Chief of Staff

SIGNED
DALE E. PEYTON
COL, GS
Assistant Deputy Chief of Staff for
Command, Control, Communications
and Computers

DISTRIBUTION: Distribution is intended for command level A.

Copy Furnished: HQ FORSCOM (AFCI-A) (record copy).

TABLE OF CONTENTS

CHAPTER 1

General

1-1. Purpose

This regulation:

a. Implements requirement in Army Regulation 190-13 for major Army command (MACOM) commanders to establish a Physical Security Program.

b. Prescribes policy/procedures and assigns responsibilities for developing and maintaining a practical, economic, and effective FORSCOM physical security program to safeguard personnel, facilities, and equipment.

c. Prescribes standards for security of specified unclassified U.S. Army assets.

d. Provides risk analysis methodology that allows commanders flexibility to tailor physical security posture and resources to meet local needs.

e. Will be used to integrate physical security efforts into Force Protection plans and procedures.

1-2. References
Required and related publications and referenced forms are listed in **Appendix A**. Prescribed forms are listed and explained in **Appendix A**.

1-3. Abbreviations and Terms
Abbreviations and special terms used in this regulation are explained in the **Glossary** at the end of this regulation.

1-4. Responsibilities
Security of the force is an operational concern with overall responsibility remaining within operational channels. Responsibilities are consolidated and listed in **Appendix B**.

CHAPTER 2
The FORSCOM Physical Security Program

2-1. Purpose
This chapter establishes and defines principle components of the FORSCOM Physical Security Program.

2-2. Standards
a. Threat Assessment: Physical Security Programs will be based upon local threat and vulnerability assessments which are updated at least annually.
b. Security Engineering: Security will be considered in standard Army design practice with security measures that are based on risk in accordance with DA Pamphlet 190-51 and threat analysis in accordance with TM 5-853-1.
c. Security Planning: Commanders will develop Installation Physical Security Plans, based on risk analysis, that are affordable, effective, and attainable.
d. THREATCON System: Physical security planning will apply specific guidance (i.e., identification of responsibilities and required resources) to the general THREATCON measures.
e. Mission Essential and/or Vulnerable Areas (MEVA): Areas which are critical to mission accomplishment or are vulnerable to theft/damage/attack will be identified and designated in order to focus security efforts.
f. Restricted Areas: Areas which are considered critical or sensitive will be identified and formally designated as "Restricted Areas" in order to give the commanders legal authority to impose special access controls.
g. Inspections: Periodic formal reviews by security specialists will be conducted in order to ensure compliance with security standards by individual MEVA.
h. Surveys: Periodic formal reviews by security specialists will be conducted in order to assess overall physical security programs.
i. Employment of Security Measures: Appropriate physical and procedural measures will be employed which provide integrated deterrence, detection, and defense capabilities in order to safeguard all personnel and material assets.

2-3. Objective
The FORSCOM Physical Security Program is an integral part of the FORSCOM Force Protection Program. It's objective is to provide commanders with guidelines and standards for planning efficient and cost-effective local physical security programs to protect assets from damage and loss. Installation physical security programs will be designed to ensure effective and efficient use of resources during peacetime to meet the threats listed below. Additionally, they will expand to allow for security measures that will include plans for security of the installation in order to permit the rapid marshaling and deployment of forces and material during mobilization, in times of national emergency, and war. Physical security programs must protect assets from the following threats:
a. Criminals
b. Disaffected persons
c. Hostile intelligence
d. Paramilitary forces
e. Protesters
f. Saboteurs
g. Terrorists

2-4. Components
Physical security is achieved through an integrated process consisting of the following basic components. Individual components are discussed in subsequent paragraphs.

a. Threat assessment (para 2-5)
b. Duty assignments (para 2-6)
c. Security planning (para 2-7)
d. Risk analysis (para 2-8)
e. Mission essential and/or vulnerable areas (para 2-9)
f. Official designation of restricted areas (para 2-10)
g. Coordination (para 2-11)
h. Councils (para 2-12)
i. Conducting inspections and surveys (para 2-13, 14 & 15)
j. Implementing security measures (para 2-16)

2-5. Threat Assessment
Physical security programs must be tailored to meet local needs. A key element of this process is assessment of the local threat. Installations, and their equivalents, will develop a local threat statement. This statement will identify local threats, and make full use of investigative resources available in the geographic area to anticipate criminal and intelligence activities that threaten security of Army property and personnel. The Physical Security Threat Assessment will be taken from the overall Force Protection Threat Statement. The local threat statement will be included in the installation physical security plan. At a minimum, liaison shall be established with the following agencies:

a. Local Federal Bureau of Investigation (FBI) field office.
b. Local civilian police and sheriffs departments.
c. Installation CID, MI and MPI agencies.
d. Local Bureau of Alcohol, Tobacco, and Firearms field office.

2-6. Duty Assignments
An effective Physical Security Program is dependent on the formal assignment of critical security related responsibilities. A listing of responsibilities is contained in **Appendix B**.

2-7. Security Planning
Commanders at all levels must plan for the security of the assets under their control. At installation and equivalent levels formal physical security plans are required. Physical security plans will tie security measures together and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. The plan must have reasonable and affordable protective measures. Requirements at different threat conditions (THREATCONS) will be identified. **Appendix D** contains a more detailed discussion of physical security plans and establishes minimum requirements for the elements of a formal plan.

2-8. Risk Analysis/Risk Management
To determine the type and extent of the commitment of resources toward physical security programs, commanders must assess the threat, vulnerabilities, available resources and the value of protected assets. The Army's five step risk management process will be utilized for physical security program design. The five steps consist of: identifying hazards, assessing the hazards, developing controls, implementing controls, and supervision and evaluation. Risk analysis is conducted to identify and assess hazards. The DA PAM 190-51 provides an in-depth discussion of risk analysis.

2-9. Mission Essential and/or Vulnerable Areas (MEVA)
Physical security MEVA are areas that are considered either mission essential or vulnerable, or both. They consist of facilities housing information, equipment, and/or personnel that are formally designated by the installation commander as requiring additional protection through application of increased physical security measures. Examples of assets that should be considered for designation as physical security MEVAs are: arms, ammunition and explosive storage rooms, facilities, or areas; airfields, aircraft parking, or aircraft maintenance areas; consolidated supply and storage operations; finance offices; IDS monitor stations; etc. Security standards for areas commonly designated as physical security MEVA are found in AR 190-11 and AR 190-51. This designation as a physical

security MEVA imposes the requirement for formal physical security inspections to be conducted by the Installation Provost Marshal or Security Office.

2-10. Restricted Areas

If access controls are required in order to safeguard assets, the area may be designated as a restricted area. Formal designation as a restricted area gives the commander legal authority to impose access control requirements deemed necessary. A "restricted area" is any area to which entry is subject to special restrictions or controls for the purpose of safeguarding assets. Forces Command utilizes three categories of restricted area; exclusion (most secure), limited (2d most secure), and controlled (least secure restricted area). The **Glossary** contains definitions of each of the above. Within the 50 United States, the authority to designate an area as a restricted area comes from Sections 793(a) and 793(b) of Title 18, United States Code and from Section 21, Internal Security Act of 1950 (64 Stat. 1005, 50 USC 797). This authority is further discussed in DOD 5200.8.

2-11. Coordination

a. The Physical Security Program requires coordination to ensure physical security plans complement each other and security efforts are synchronized. In developing a security plan, coordination and close liaison must be conducted. To the extent permissible, such interaction should allow for an exchange of intelligence, information on security measures being employed, contingency plans, and any other information to enhance security. On an installation, the host activity will assume responsibility for coordinating physical security efforts of all tenants, regardless of the DOD components represented, as outlined in the support agreements and the host activity security plan. The purpose of such coordination is protection in depth. Authority, jurisdiction, and responsibility must be set forth in a manner that ensures protection and avoids duplication of effort.

b. Construction projects require coordination between security specialists and engineers. Coordination must span the complete timeline from construction planning through completion of the project.

c. Coordination must be on-going between security specialist and resource management personnel to ensure continued availability of funds for security purposes.

2-12. Councils, Working Groups, Fusion Cells and Committees

a. Certain groups are established at the MACOM and Installation level to ensure coordinated efforts in the implementation of Force Protection and Physical Security requirements. Army Regulation 525-13, The Army Antiterrorism Program, and Army Regulation 190-13, Physical Security, contain guidance for the appointment and responsibilities of committees, councils and fusion cells.

b. Installation planning boards will include a physical security representative. The representative will ensure that the provisions of the physical security regulations are considered and made a matter of record during the planning process.

2-13. Physical Security Inspections

a. The FORSCOM Physical Security Inspections will be conducted IAW AR 190-13, para 2-11.

b. Where available, inspections will be conducted utilizing the Security Management System (SMS).

2-14. Physical Security Surveys

a. The FORSCOM installations will complete an installation physical security survey (PSS) on at least an annual basis. Surveys may also be appropriate when a significant change in the threat or mission occurs.

b. A completed PSS provides a formal, recorded review of an installation's physical security program. [See paragraph "e" below for discussion of a "completed" survey.] The PSS provides the Commander with an assessment of the overall security posture of the installation. The completed survey will outline the installation physical security program's strengths and weaknesses and provide recommended actions for the application of resources, in a prioritized manner, for the reduction of vulnerabilities. The PSS will be reviewed by the Installation Fusion Cell/Force Protection Committee on an annual basis in conjunction with the submission of the annual Installation Force Protection Status Report required by the FORSCOM Force Protection OPORD.

c. The FORSCOM Form 190-R will be used to record physical security survey data. This form may be modified to cover unique command requirements. A copy of the form for reproduction purposes and instructions for completion of the form are located at **Appendix A**. Survey data will be continuously maintained and updated as needed. Data collected on this form provides a basis upon which to complete the survey as discussed in paragraph "e" below.

d. Specific areas evaluated in a PSS include:

(1) Identification of any security vulnerabilities based on current threat assessment.

(2) Identification and prioritization of MEVAs and HRTs.

(3) Identification of existing security deficiencies. (Waivers, exceptions, pending security related engineering work orders and crime trend indicators).

(4) Status of law enforcement and security forces.

(5) Status of Intrusion Detection Systems (IDS).

(6) Status of security plans.

(7) Review of threat assessment procedures.

(8) Review adequacy of current threat statement.

e. The form serves only as a means for collecting pertinent data, it by itself does not complete the survey requirement. Once the survey form has been completed, it will be used as the basis for a report from the Installation Provost Marshal or Security Office to the Installation/Activity Commander. The completed survey will consist of a cover memorandum to the Commander, which summarizes the physical security posture of the installation as discussed above; the completed DA Form 2806-R, FORSCOM Form 190-R, with enclosures; and any necessary exhibits. Examples of exhibits include maps, photographs, sketches, charts, etc. Exhibits will assist in clarifying findings and recommendations, and assessing their criticality and degree of vulnerability.

2-15. Security Engineering Surveys

Security Engineering Surveys are the process of identifying, by means of an on-site survey, physical security related engineering requirements associated with facility enhancements for physical security and Force Protection, including IDS installation. Security engineering surveys will be performed when planning any new construction or renovations to existing facilities where there are likely to be physical security requirements. See Appendix 1 to Annex O, OP-ORD 1-98.

2-16. Security Measures

Security measures consist of procedures which enhance security and physical assets such as lights, fences, alarms, etc. which are employed to enhance security. Security measures deter, detect, and defend (delay or defeat) the threat. Deterrence is enhanced when measures employ randomness and are highly visible. Security measures should be integrated and layered. **Chapter 4** outlines the minimum security measures required for selected categories of Army assets for which FORSCOM standards have been added. Additionally, selected AA&E storage standards have also been outlined.

CHAPTER 3

Electronic Security Systems

3-1. Purpose

This chapter:

a. Prescribes policy, responsibilities, standards, and procedures for selecting, acquiring, and using electronic security systems (ESS) within FORSCOM.

b. Will be used to develop intrusion detection systems (IDS) programs.

c. Does not include ESS procedures for cryptological facilities (SCIFs), those procedures are outlined in AR 380-5 and DCID 1/21.

3-2. Physical Security Equipment Overview

a. As defined in TM 5-853-4, Electronic Security Systems (ESS) include intrusion detection systems (IDS), closed-circuit television (CCTV) and entry control systems (ECS). These systems can be used as measures to enhance a facilities' physical security posture.

b. When properly designed, installed, and maintained, ESS technologies are valuable additions to FORSCOM and individual command physical security programs. Effective employment of ESS requires a total system approach which integrates policy, procedures, equipment, protective construction, and awareness. This requires a coordinated effort by the employing unit and the supporting physical security office, DPW, DOIM, and DOL.

c. Electronic systems may reduce guard requirements by providing cost-effective continual surveillance, detection, assessment, delay, response and/or access control protection.

d. A basic IDS consists of a sensor connected to a control unit. This control unit is linked to a monitored annunciator console. The IDS is supported by a security response force. The IDS is useless unless it is properly operated, monitored and supported by prompt security force action when the system is activated.

3-3. Planning Guidelines

Paragraph 4-15, AR 190-13 discusses planning for ESS/IDS. Intrusion detection systems and other ESS applications are planned, budgeted, procured, and initiated the same as other Army systems. Paragraph 4-16, AR 190-13 and paragraphs 3-6 through 3-12 of this regulation discuss project submission and acquisition procedures.

a. The ESS equipment projects are initiated:

(1) As the result of a physical security survey, risk analysis, or inspection identifying vulnerabilities which can be reduced by the installation of ESS.

(2) To comply with regulatory requirements.

(3) To satisfy security requirements identified during the design of Military Construction Army (MCA) projects.

(4) To satisfy security requirements identified during the design of Operations and Maintenance Army (OMA) funded renovation projects. Such projects may require the programming of OPA-3 funds if new equipment must be purchased.

(5) To employ ESS as an alternative to guards as a means to ensure continuous surveillance or maintain access control.

(6) To consolidate alarm monitors to conserve manpower.

b. Use of other than Integrated Commercial Intrusion Detection System (ICIDS) or Joint-services interior intrusion detection systems (J-SIIDS) components to satisfy IDS requirements requires approval by Commander FORSCOM OPM, ATTN: AFPM-FP, 1777 Hardee Avenue, SW., Fort McPherson, GA 30330-1062. The FORSCOM OPM will not consider approval of commercial intrusion detection systems (CIDS) unless:

(1) The system requirement(s) exceeds the capabilities of the Alarm Monitor Group (AMG), 25 to 64 zones.

(2) The system supplements an existing commercial system.

(3) The proposed system requires exterior sensors.

(4) There is an architectural or technical problem with installing J-SIIDS.

(5) The CIDS would be more cost-effective than using ICIDS or J-SIIDS.

(6) A low priority non-appropriated fund requirement is involved.

c. Programming IDS for MCA projects.

(1) When an MCA project requires a J-SIIDS, ICIDS or CIDS, provide an estimate of the required installation funds as a line item on the front page of DD Form 1391 (FY##, Military Construction Project Data) submitted to DA for approval. If IDS installation funds were omitted from DD Form 1391, a user change request for the IDS will be submitted to the MACOM.

(2) Include OPA-3 funds for the purchase of CIDS with other OPA funds.

d. Programming Installation funds.

(1) Except for MCA projects, IDS installation must be accomplished with OMA FUNDS. Purchase of ESS in excess of $100K requires OPA3 funding. Budget Activity 11 (BA11) mission funds may be used for J-SIIDS installation only with FORSCOM PM approval. Installations will request OMA funds for ICIDS add-ons or other changes after initial installation has been completed.

(2) Installations will request OMA funds for maintenance and integrated logistics support of ESS systems.

(3) Installation Physical Security Office, will ensure ESS/PSE acquisition, maintenance and monitoring requirements are included on their annual MDEP RJC6 submissions for their installation OMA forecast.

3-4. Priorities

Priorities for IDS or other ESS installations depend on the asset, type of facility, and degree of protection required. Arms, Ammunition and Explosives (AA&E) IDS requirements are listed in AR 190-11. Additional guidance concerning other facilities where IDS should be integrated into the total security system is contained in AR 190-13, para 4-10. Priorities for installation will be consistent with the guidance outlined in AR 190-13, para 4-9.

3-5. Risk Analysis

Installation Physical Security will conduct risk analyses in coordination with local security managers, organization commanders or facility managers. Integral to the risk analysis are threat assessments, normally provided by supporting military intelligence units and CID. Units will request risk analysis IAW the guidelines established in AR 190-51, para 2-2. The results of the risk analysis will be used during planning to identify, assess, and validate physical security requirements to include the need for ESS/PSE.

3-6. Forecasting

a. Installation Physical Security must forecast IDS and other ESS technology applications and costs before acquisition. Forecasting ensures the availability of components and funds when the IDS is required. Forecasts will cover a 7-year period by fiscal year. This is mandated by law, it supports the Program Objective Management (POM) and Future Year Defense Plan (FYDP). The forecast must identify the project; location and unit project supports; fiscal year required; justification; priority code IAW AR 190-13, para 4-9; Operations and Maintenance Army (OMA) funds necessary to reimburse design, site preparation, and installation costs; and Other Procurement Army (OPA-3) funds necessary for equipment procurement. Include with the forecast a consolidated equipment list which indicates, by fiscal year, the quantity of each J-SIIDS component required.

b. Installation Physical Security will coordinate forecasts with the supporting DPW, DRM, and DOIM. Installations will consolidate, review and prioritize forecast requirements IAW AR 190-13, para 4-9, before submission to FORSCOM OPM.

c. Forecast submissions alone do not constitute approval for IDSs. A site survey is required prior to final approval for funding. The results of the site survey are required to support the project request packet, which must be submitted to FORSCOM OPM as specified in paragraphs 3-9 and 3-10 of this regulation.

d. On annual forecasts, installations will note any previously forecasted projects no longer required, any projects suspended to another fiscal year, and any changes in funding or equipment requirements.

e. All J-SIIDS should be programmed for replacement between 10 to 15 years after initial installation or last life cycle replacement date. The service life varies from system to system. The servicing DPW will determine the replacement date.

f. Intrusion detection system/physical security equipment technologies not forecasted, but required immediately, may affect forecasted projects. A project request packet, prepared IAW para 3-9 and 3-10, must be submitted through FORSCOM OPM to obtain funding approval. Submission of unforecasted requirements (UFR) must include documentation of extenuating circumstances preventing forecasting.

3-7. Identification and Verification of Requirements

Installation Physical Security will identify and verify IDS requirements based on the following:

a. Requirements and priorities from applicable regulations
(for example, AR 190-11, AR 190-13, AR 190-51, and AR 525-13).

b. The FORSCOM Force Protection OPORD.

c. Latest physical security inspections, surveys, and risk analyses (see AR 190-51).

d. Crime statistics.

3-8. Coordination

a. Site surveys must be conducted and submitted to FORSCOM OPM (AFPM-FP), for approval. Site surveys are required prior to final approval of funding. Installation Physical Security will coordinate completion of a site survey according to the U.S. Army Corps of Engineers (Huntsville District) Procedures Guide for Intrusion Detection Systems, or other applicable electronic security system survey guides, with:

(1) Director of Public Works (DPW). Request DPW assistance for design, estimates, and installation, by submitting a DA Form 4283 (Facilities Engineer Work Request).

(2) Area Director of Information Management (DOIM) representative. Request in writing the DOIM provide assistance to coordinate communication media.

(3) Director of Logistics (DOL). Request in writing that the DOL provide assistance for equipment procurement and property book accountability.

b. Extensive or complex commercial technology projects may require the expertise and participation of the Huntsville Division IDS Technical Center of Expertise (IDS MCX) to properly complete the survey. Requests for such assistance must be coordinated with FORSCOM, ATTN: AFPM-FP, 1777 Hardee Avenue, SW., Fort McPherson, Georgia 30330-1062.

3-9. Project Request Packet for J-SIIDS Projects

A project request packet with the following information must be sent through the Installation Physical Security, with review and endorsement by the DPW, DOIM, and DOL, to FORSCOM OPM.

a. Request for system approval.

b. Photocopies of all equipment requisitions DA Form(s) 2765-1 or DA Form(s) 1348-6 completed IAW DA Pam 710-2-1.

Note: The J-SIIDS end item components are furnished free as initial issue to user installation(s), the components are paid for with OPA-3 funds from U.S. Army Communications and Electronics Command (CECOM). However, J-SIIDS replenishment components and repair parts must be funded by the user installation from OMA funds.

c. Statement identifying the basis for project submission. The statement should clearly identify that the project was submitted to satisfy a regulatory requirement (include citation which identifies the applicable Army Regulation number and paragraph citation down to the lowest sub-para which contains the requirement), reduce a vulnerability identified during a risk analysis or physical security survey, or produce manpower savings.

d. Designated security level of facility, as defined in para 4-10, AR 190-13.

e. List of materials, to include cost estimate for system installation. (See, DEH Automated IDS Cost estimator CEHND-SP-93-268-ED-ME)

f. A completed site survey and engineer blueprints or drawings of the protected area and component locations.

g. Projected fiscal year for system installation.

h. A request for Operation and Maintenance, Army (OMA) funds to reimburse design, site preparation and installation of the system.

i. A statement that BASOPS funds are available for maintenance of the system.

j. Additional information supporting the IDS requirement (for example, physical security inspections or surveys).

3-10. Project Request Packet for Commercial Technologies

If conditions of para 3-3 of this regulation exist, send a project request packet through Installation Physical Security to FORSCOM OPM. The packet must include the following information:

a. A request for system approval and funding (to include cost estimates for purchase and installation).

b. Point of contact and telephone number and a funding authority to receive DD Form 448 Military Interdepartmental Purchase Request (MIPR) from U.S. Army Communications and Electronics Command (CECOM).

c. Statement identifying the basis for project submission. The statement should clearly identify that the project was submitted to satisfy a regulatory requirement (include citation which identifies the applicable Army Regulation number and paragraph citation down to the lowest sub-para which contains the requirement), reduce a vulnerability identified during a risk analysis or physical security survey, or produce manpower savings.

d. Designated security level of facility, as defined in para 4-10, AR 190-13.

e. Justification as to why J-SIIDS/GFE security equipment cannot meet requirements.

f. Justification as to why an existing system cannot be expanded, if the selected CIDS requires an additional monitor panel.

g. A completed site survey, technical specifications of proposed components, and engineer blueprints or drawings to scale of the system (protected area and component locations).

h. Projected fiscal year for system installation.

i. A statement that Installation BASOPS funds are available to maintain the system.

j. Other information supporting the requirement (for example, physical security inspections or surveys).

k. Security Engineering Surveys which are beyond local capability may be requested through FORSCOM OPM and accomplished on a reimbursable basis by USACE (Protective Design and/or Intrusion Detection Systems Mandatory Centers of Expertise).

3-11. Technical Review for Commercial ESS

a. Requests for purchase, lease, or lease renewal of commercial ESS to include; electronic entry control devices, and closed circuit televisions (CCTVs) (if connected to an IDS and used in a surveillance or assessment mode) will be sent through Physical Security channels to the FORSCOM PM. The OPM will forward technology designs to USA CECOM (PSEMO) 5900 Putman Road, Ste 1, ATTN: AMSEL-DSA-PSE, Fort Belvoir, VA 22060-5420. The PM-PSE will review to ensure the design integrates compatible equipment components to produce an operating unit capable of providing total, reliable, and continuous monitoring. The review considers the following:

(1) Evaluation of physical security requirements to determine if the system or equipment will significantly improve protection.

(2) Evaluation of the technical specifications and design of requested CIDS/CPSE technologies to determine suitability for use with other DOD standardized systems or commercial systems already in use or under development.

(3) Evaluation to ensure the requested system counters the threat without unnecessary expenditure of funds.

b. Commercial ESS technologies may be approved if it is determined that DOD standardized equipment is not reasonably available, is not cost-effective, or does not meet the requirements of a particular facility.

c. Technical review of standardized physical security equipment (i.e., J-SIIDS) is not required.

3-12. IDS Acquisition Procedures

a. Under no circumstances will installations procure or allow security technologies to be installed without FORSCOM Provost Marshal approval. The FORSCOM Provost Marshal will review system requests/submission packets in coordination with ODCSENG.

b. Joint Services Interior Intrusion Detection Systems (J-SIIDS), installation customers/users will prepare requisitions in accordance with AR 725-50 and submit requisitions through the appropriate DOL property book officer (PBO). Initial issue items are funded by CECOM and are at no cost to the user for new installation. Installation customers/users must pay for replacement of non-expendable components.

c. Commercial IDS (CIDS) or other commercial Electronic Security Systems (ESS) that has been approved by FORSCOM, the installation DPW will initiate procurement using negotiated procurement procedures.

3-13. Physical Security Plans

a. Installation physical security plans will identify IDS locations and include the following:

(1) Type of area or structure being protected.

(2) Type of sensors used.

(3) Type response forces required and source providing the response forces.

b. Detailed instructions concerning monitoring procedures, response force procedures, testing and inspection requirements, actions in the event of power failure, and identification of auxiliary power sources will be included in an annex to the Force Protection Plan and/or Installation Physical Security Plan.

c. Associated with the physical security plan, the Installation will maintain an IDS/ESS database which includes the following:

(1) Using unit.

(2) Building, room number and type facility protected.

(3) Date of installation or life cycle replacement.

(4) Facility priority code IAW para 4-9, AR 190-13.

(5) Monitor location.

(6) Monitor personnel.

(7) Type system.

(8) Manufacturer name.

(9) Type sensors in use.

(10) Source providing Response Force.

3-14. IDS System

a. System Overview. The IDS consists of intrusion sensors connected to a monitor cabinet backed by a security response force. Intrusion sensors detect through sound, vibration, motion, electrostatic emissions, and light beams. Information concerning categories of sensors and their recommended use is contained in **Chapter 7**, FM 19-30. Technical criteria is provided in TM 5-853-4.

b. Categories of Sensors.

(1) Penetration Sensors. Sensors that detect penetration of a protected area, including entry through doors, windows, walls, floors, ceilings, and other openings in a room.

(2) Volumetric Sensors. Sensors that detect the movement of an object inside a protected area.

(3) Duress Switches. Switches that are activated by an armorer, employee, duty personnel, guard, or protected person to call for assistance.

(4) Point Sensors (Magnetic Sensors, Capacitance Proximity Sensors). Sensors designed to detect the attempted removal of an item from its normal position within the protected area (for example, weapons racks, storage cabinets, safes, security containers, desks).

3-15. Recommended Sensors

a. Balanced magnetic switches are the recommended primary sensors for detecting the opening of doors and windows. These switches are used in conjunction with passive ultrasonic or passive infrared sensors secured to ceilings, walls, and floors.

b. Grid wire sensors or vibration sensors may be used for securing floors, walls and ceilings, and openings such as doors and windows.

c. Capacitance proximity sensors may be used for detection inside a facility and are recommended to protect class 5 weapon containers.

d. Duress alarms **will** be used in all arms rooms and may be used in other areas, if required, in conjunction with balanced magnetic switches and motion sensors, to provide a means of signaling a response force in a robbery or duress situation.

3-16. Description of System Components

Technical Manuals (TMs) 5-6350-264-14-1 and 5-6350-264-14&P-2 through 5-6350-264-14&P-13 identify the individual components that form a J-SIIDS. The TM 5-6350-280-23&P and TM 5-6350-280-10 address the Alarm Monitor Group. Comparable CIDS components must meet or exceed the criteria in applicable TMs. Listings/ applications of other available government furnished physical security equipment components/systems can be obtained from CECOM.

3-17. Location of IDS Components

Selection and application of J-SIIDS are prescribed in Technical Bulletin (TB) 5-6350-264. The ESS must meet or exceed the criteria in TB 5-6350-264 and TM 5-853-4. Commercial sensors should follow ICIDS-II Functional Purchase Descriptions (FPDs) for ICIDS commercial sensors. Refer to ICIDS-II Selection Application Installation Guide (SAIG). Additional guidance is as follows:

a. Sensors should be positioned in protected areas at locations providing maximum protection. Enough sensors should be used to ensure the entire area is protected without operating the sensors at maximum sensitivity.

b. The control unit normally will be mounted on the interior wall of the protected facility (excluding Class V weapons containers) as close as possible to the main entrance. Control units may be mounted on the outside of ammunition and explosive storage structures if they are secured inside a locked security container.

c. The monitor cabinet should be positioned to ensure the status displayed is not obstructed from the continual view of monitor personnel. A required location for the monitor station is not specified because IDS locations must be evaluated individually and locations approved by the respective commander.

d. The duress alarm (commercial or J-SIIDS alarm latching switch) will be positioned inside the protected area at a location where it is readily available to on duty personnel and can be operated without being observed by an intruder. The preferred location is on the floor under issue windows. If issue windows are not used, the switch should be located under the armorer's desk or on the floor adjacent to the main entrance door frame.

e. When installed at designated sites, the audible alarm will be located on the outside of the protected area and mounted as high as possible on the protected structure wall or utility poles. This will prevent tampering and increase the sound effect. The audible alarm must be accessible to maintenance personnel.

3-18. System Wiring Diagram

A system installation wiring diagram and grid wire dimensional diagram will be made for each protected area. The diagrams indicate which sensors are installed and show color-coded interconnections between each sensor and the control unit. System options (for example, alarm option, length of time delays, type of monitor to which the module system reports, signal transmission option) should be indicated on the diagram. The diagram will serve as an aid to maintenance personnel when repairs are needed. Wiring diagrams or other instructions developed by the installer to assist maintenance personnel will be kept inside the control unit. System wiring diagrams and associated site specific information must be classified at the classification of the level of the area protected. The minimum classification level will be “For Official Use Only.”

3-19. Transmission Lines and Backup Power

In FORSCOM, if undetected access to transmission lines between the control unit and monitor cabinet is possible, line supervision will be provided. Signal transmission line supervision is a technical electronic safeguard to monitor whether an electrical circuit has been broken, grounded or shorted. If undetected access between the sensors and control unit is possible, wiring will be contained in rigid conduit or EMT will be used. Class B lines, lines that are

not supervised, and systems that do not conform to the above will be upgraded. A backup power source or uninterruptable power supply will be provided for each control unit and monitor cabinet and must be capable of lasting at least 4 hours or 24 hours for off-post USAR facilities.

3-20. Installation

a. Planning for ESS technology applications must include coordination with the local area DOIM representative to ensure data transmission have line compatibility. Coordination will ensure the availability of dedicated transmission media when installation begins.

b. Installation Physical Security will ensure that only trained and qualified personnel install IDS/PSE. The DPW personnel will install IDS/PSE technologies unless installation is to be performed by contract. The TMs 5-6350-264-14-1 and 5-6350-264-14&P-2 through 5-6350-264-14&P-13 explain how to install J-SIIDS components.

c. Contractor-installed IDS/PSE technologies will be inspected by trained or certified DPW/DEH personnel before the installed system is accepted. Performance criteria required for acceptance of CIDS/commercial security technologies will meet or exceed the criteria in applicable TBs and TMs. The ICIDS and other commercial IDS require a certified System Administrator.

d. In accordance with paragraphs 4-13b and c, AR 190-13, a post completion evaluation may be requested from the IDS Mandatory Center of Expertise (Huntsville), to ensure the IDS was properly installed and is being maintained at the appropriate level. This evaluation is required for CIDS/CPSE projects. Funding for this evaluation must be programmed through FORSCOM PMO and will be included in OMA forecasts.

3-21. Personnel Suitability and Reliability Checks

a. Requirements for personnel suitability checks and clearances will be clearly stated in contracts.

b. Commanders may develop command-oriented background check requirements consistent with the local threat situation, sensitivity of the facilities protected, and the vulnerability of the facilities served.

3-22. IDS Operating Procedures

a. Two people are usually required to operate an IDS; one at the control unit and the other at the monitor cabinet. The monitor station operator must be a responsible person who can alert a security or response force during an alarm. The control unit operator must be the person designated to unlock and lock the protected area. The operator contacts the monitor station operator to verify the protected area is being opened or secured.

NOTE: The ICIDS does not require the control unit operator contact the monitor station operator. The control unit operator interfaces with the central computer by utilizing a PIN to provide access/secure status to the zone being protected and does not normally interact with the monitor station operator.

b. The three basic modes of IDS operation are:

(1) Secure. The IDS are operated in the secure mode when a protected area is secured or is not open to authorized personnel. Alarms (intrusion, tamper, and duress) are processed and routed to the status modules. Alarms, except the duress alarm, are routed to an audible alarm, if used. An exit time delay is provided to allow authorized personnel to turn the control unit mode switch to secure and leave the protected area without creating a latched alarm. The ICIDS and other CIDS utilize a key pad and do not use control unit mode switches.

(2) Access. The IDS are operated in the access mode when a protected area is open to authorized personnel. IDS are set to prevent intrusion alarms from being routed to the status modules and the audible alarm. Tamper and duress alarms are routed to the status modules, but only tamper alarms are routed to an audible alarm. An entrance time delay is provided to allow authorized personnel to enter the protected area and turn the control unit mode switch to access without triggering an audible alarm or activating the status module alarm. The ICIDS and other CIDS utilize a key pad and do not use control unit mode switches.

(3) Test/Reset. The test/reset mode is used when maintenance is being performed on a system. In this mode IDS are set to prevent alarms from being routed to the audible alarm, rather they are routed to status modules. On receiving alarm input, an audible signal in the control unit is activated for 10 seconds as an aid to IDS testing. If the mode switch is placed momentarily in the test/reset position, the audible alarm is reset and silenced. If the mode switch is switched from the test/reset position to the secure position, all processed alarms are cleared if the sensor inputs have ceased to be alarmed. The ICIDS and other CIDS utilize a key pad and do not use control unit mode switches.

c. The monitor console operator and control unit operator will use duress procedures. Supervisory personnel will establish duress procedures for use at the monitor cabinet location. Procedures should be changed at least quarterly or when a security compromise is suspected. Only personnel involved in opening or securing the protected area and monitor personnel should have access to duress procedures.

d. Intrusion detection system sensors will activate at the monitor station. A duress alarm at the monitor console will be relayed to response forces by the monitor operator using the fastest means available (preferably direct voice communication). If possible, the monitor station should be located with the response force.

e. Monitor stations will be staffed continuously to ensure fast response to alarm conditions. Monitor personnel will not be assigned any additional type of duty that diverts their attention from the monitor console.

3-23. Record Keeping

DA FORM 4930-R (Alarm/Intrusion Detection Record) will:

a. Be used to log daily IDS operations. For computer-driven monitors that provide a printout of system activity, only information not on the printout need be entered on the DA Form 4930-R (for example, weather, patrol dispatch, time to clear).

b. Include at least the following information -

(1) Time.

(2) Date.

(3) Location of alarm.

(4) Identity of the person receiving the alarm.

(5) Cause of the alarm.

(6) Action taken in response to the alarm.

c. Be maintained at the monitor station for 60 days after the last entry and destroyed thereafter unless required for investigative purposes.

3-24. Maintenance

Installation Physical Security will ensure that only trained and qualified personnel maintain IDS/ESS. Trained or certified DPW/DEH or DOL personnel perform maintenance of ESS unless maintenance is performed by contract. The TM 5-6350-264-14-1 provides guidance on maintenance of J-SIIDS components.

a. Unit level maintenance is restricted to general cleaning type maintenance (for example, dusting and wiping clean the exterior portion of IDS components with a dry cloth). Do not paint IDS components.

b. Contractor-installed ESS will be maintained as specified in the Government maintenance contract. The contractor should be required to perform routine maintenance inspections no less than 6 month intervals.

c. Organizational personnel will perform periodic preventive maintenance checks and services. Conditions requiring repair will be reported to DPW/DEH/DOL within 2 hours for corrective action. The DPW/DEH/DOL will make necessary repairs as soon as possible. The IDS required by regulation should be repaired within 6 hours during normal duty hours and within 24 hours during normal non-duty hours to avoid excessive security manpower requirements.

3-25. Logistics Procedures

a. Installation DPW/DEH/DOL are responsible to maintain, repair, and stock expendable repair parts for IDS.

b. Supporting maintenance activities will order and stock only those expendable repair parts needed to perform J-SIIDS maintenance and repair.

c. Initial requisitions for new GFE IDS accountable components are submitted through the servicing installation property book officer (PBO).

d. The GFE IDS users will initiate requests for replacing unserviceable GFE IDS equipment sets declared as nonexpendable items coded “N” in the Army Master Data File (AMDF). Users will submit requests for supply action and provide applicable fund citations. After receipt, GFE IDS users (requisitioner of the end item) will submit a request to the DPW for quality surveillance (bench check) and installation of the equipment.

e. If J-SIIDS components fail on initial installation, procedures in AR 702-7-1 will be used, and a Standard Form (SF) 368 (Product Quality Deficiency Report) will be submitted by DEH. Each end item or repair part failure is an individual action and must be treated as such. Procedures in AR 710-2, DA PAM 710-2-2 and AR 725-50 will be used by DOLs to requisition replacement parts for faulty components.

f. Government Furnished Equipment users will maintain PMO approval documents, requisitioning information (such as complete requisition numbers, date of order, listing of components) and any other information necessary to

track the procurement process effectively. Requesters will make periodic checks with their servicing DOL to check the status of ordered equipment.

g. The IDS component accountability will be maintained in accordance with AR 710-2, DA PAM 710-2-1 and AR 735-5.

h. The DPW is responsible for maintaining IDS drawings and updating the drawings when changes occur.

i. Installations must ensure maintenance contracts or other methods are in place to ensure ICIDS/CIDS systems are properly maintained.

3-26. Response to Alarms

a. General. Installation Directorate of Public Safety or Physical Security Officer establishes alarm response policy. The policy, implemented through local Force Protection and Crisis Management Plans, must include designation of response force type, size, armament, etc.

b. Use of Force. Installation Public Safety Officer or Physical Security Officer will establish procedures on the use of force according to AR 190-14.

c. Duties. The response force will observe, report, and take action as directed by the response force commander. The response force must:

(1) Be located so it can respond promptly to an activated alarm. In no case will arrival at the scene exceed 15 minutes from alarm activation.

(2) Go to the protected area and determine the cause of the alarm. A telephone call to the protected area is not an acceptable response when an alarm sounds.

(3) Neutralize an actual alarm condition of any alarm in the protected area (d below).

d. Response Procedures. The procedures in (1) through (6) below are recommended when an alarm is received from a protected area.

(1) When an alarm is announced at the monitor station, the operator will notify the response force commander and the MP desk sergeant and give the location and time of the alarm.

(2) The response force will be sent to the building or site where the alarm has been activated.

(3) The response force will block all entrances and exits. One or more members of the response force will be posted at each entrance as they arrive or as instructed by the senior response force member. No one will be allowed to enter or exit the building.

(4) The senior response force member will supervise a search of the protected area to determine whether or not an intrusion or attempted intrusion has occurred. If there are no signs of a break-in, the senior response force member will inform the monitor station operator and MP desk sergeant, and normal duties will be resumed.

(5) If an intrusion has occurred or was attempted, the senior response force member will inform the monitor station operator and the MP desk sergeant, and temporarily detain witnesses or suspects until informed of the action to be taken by the response force officer in charge (OIC) or noncommissioned officer in charge (NCOIC). The response force OIC or NCOIC will secure the area and request MP assistance to summon the appropriate investigative agency (for example, CID or military police investigator).

3-27. Inspections

Physical security inspectors will:

a. Conduct an IDS systems check during security inspections and surveys required by ARs 190-11 and 190-13.

b. Conduct operations and functions inspections of IDS during scheduled physical security surveys and inspections to ensure sensors, signal processors, control units, and monitor consoles/cabinets work. Inspectors will use available installation manuals, contract statements of service, and modification work orders for this purpose.

c. Visually inspect components and conduits for evidence of tampering.

d. Physical Security inspectors will also review engineer drawings of the various zones to ensure sensor and control unit locations are as indicated on the drawings.

3-28. Access Roster

a. A roster of personnel authorized to open and secure the protected area will be provided to the monitor station. The roster will indicate name, social security number, and telephone number of personnel at the protected area. The commander of the protected area will sign the roster. The roster will be kept where it is readily available to the monitor station operator and out of sight to unauthorized personnel.

b. Installation Physical Security will obtain the list of trained and qualified IDS/PSE equipment installation and maintenance personnel from appropriate activities, verify their security screening, and provide this list to the monitor

station and protected areas. The installation security manager will verify and authenticate the roster. The roster will indicate name, social security number, security clearance or background/records check as applicable and telephone number of authorized personnel. Only personnel who have had favorable checks will be included on the roster. To prevent unauthorized tampering with IDS, only personnel listed on this roster are permitted to perform maintenance.

3-29. Key Control
During initial installation and test phase of IDS, the installing activity will maintain key control. On completion of the final test and acceptance of the IDS, control and accountability of IDS keys become the responsibility of the unit or activity commander. Keys will be controlled IAW AR 190-11, para 3-8 and AR 190-51, **Appendix E**.

3-30. Movement of IDS Components or Systems
a. Installed IDS is "personal property, equipment in place" and must be accounted for on unit and installation property books.
b. Activity and facility closure and organization moves and inactivation's may invalidate the need for certain IDS. Commanders, in coordination with the supporting DPW, will identify inactive IDS which may be laterally transferred to other locations. The IDS components removed from closing installations will be turned in to installation Property Book Officers. Installations may keep removed components, if needed, to back fill outstanding requisitions or to fill maintenance float densities. Disposition of excess components will be coordinated through the DOL. Sufficient advanced planning will be taken to program for the ICIDS or CIDS contractor to remove and/or install a zone without invalidating warranty or life cycle contractor logistics (LCCS).

CHAPTER 4
Security Standards

4-1. Purpose
This chapter provides policy and procedure for safeguarding Army assets. This section summarizes security requirements from AR 190-11, 13, 16 and 51 and establishes FORSCOM minimum security standards.

4-2. Implementing Guidance
Not all assets can or should be given the same level of security. Efficient and cost-effective security is achieved by using resources based on local threat assessment and risk analysis. Security resources (manpower, equipment and money) are limited and must be used in response to the criticality of the asset and the risk to or vulnerability of the protected asset. This chapter contains only minimum standards at the various risk levels, local commanders are responsible for determining increased security measures, as necessary, to meet local conditions. When employing security measures, to the extent possible; use a mix of measures, layer the protection, and employ measures at random.

4-3. Waivers and Exceptions
Installation Provost Marshal Offices will submit requests for waivers and exceptions to the physical security requirements of this regulation to the CDR, FORSCOM, ATTN: AFPM-FP, 1777 Hardee Avenue, SW., Fort McPherson, GA 30330-1062.

4-4. Minimum Security Standards
a. The purpose of these tables is to clearly identify the security requirements for various categories of Army assets. Listed below are the minimum security standards (requirements) for selected categories of Army property as extracted from applicable regulations. Additionally, FORSCOM specific requirements are established and identified (FORSCOM Reg 190-13). The DA requirements are in abbreviated form, you must refer to the referenced source for the full explanation.
b. In paragraph 4-4.d. and 4-4.e, the various categories of property are identified. A detailed list of required security measures, per category, is provided in subsequent tables.

c. Some categories of assets are protected depending on the level of risk, others (such as AA&E) are protected at an absolute standard - regardless of risk. The determination of appropriate risk levels requires performance of a risk analysis IAW DA Pam 190-51, Risk Analysis for Army Property. Local plans must take into account the existing THREATCON when determining the risk level to which protection will be provided.

d. Below is an index of tables containing categories of assets that are protected based on an analysis of the existing risk. Risk levels are classified as either I, II or III. Risk level III requirements are the most stringent. Tables do not include all categories of property listed in AR 190-51, those categories for which FORSCOM standards have been added are listed.

Table 4-1: Aircraft, AC Components and Aviation Facilities

Table 4-2: Unarmed Vehicles

Table 4-3: Armed Vehicles and Towed Weapons Systems/Components

Table 4-4: Night Vision Devices and other Communications and Electronics Equipment

Table 4-5: Headquarters

e. Below are categories of assets that are protected based on an absolute minimum standard that does not vary based on risk. The AA&E security standards are based on AA&E categories established in AR 190-11.

Table 4-6: Unit Arms Rooms

Table 4-7: AA&E in Bulk Storage

Table 4-8: AA&E in Transit (by non-commercial motor vehicle)

Table 4-9: AA&E in Transit (by rail)

TABLE 4-1. AIRCRAFT, COMPONENTS & AVIATION FACILITIES

a. Risk Level I

1. Lock aircraft ignition & doors ..... AR 190-51, para 3-3e

2. Control ignition/door keys .....AR 190-51, para 3-3e

3. Park in most secure hanger or structure available, otherwise, park AC in proximity to each other and away from perimeter .....AR 190-51, para 3-3e

4. Have a written Security Plan .....AR 190-51, para 3-3f

5. Appoint a Physical Security Officer .....AR 190-51, para 3-3f

6. Conduct security check every 4 hours .....AR 190-51, para 3-3f

7. Control access at all times .....AR 190-51, para 3-3f

8. Designate airfield as "restricted area" .....AR 190-51, para 3-3f

9. Prohibit POV parking .....AR 190-51, para 3-3f

10. Secure accessory equipment such as boarding ladders, vehicle tugs, etc. .....AR 190-51, para 3-3f

11. Close coordination with local authorities .....FORSCOM REG 190-13

12. Have communications with response & police forces ....FORSCOM REG 190-13

13. Have an active countersurveillance program .....FORSCOM REG 190-13

**********(Aircraft with AA&E Aboard)**********

14. Park in lighted area .....AR 190-51, para 3-3b

15. IDS or continuous surveillance .....AR 190-51, para 3-3b

16. When possible, remove weapons to secure storage area or make inoperable .....AR 190-51, para 3-3b

*********(Aircraft with missiles/rockets in ready to fire configuration)*********

17. Provide 24 hour armed guard surveillance .....AR 190-11, para 5-8c

**********(Aircraft with classified equipment)**********

14. See AR 190-51, para 3-3d.

b. Risk Level II

1. All requirements from Level I

2. Protect with perimeter fencing .....AR 190-51, para 3-3e

3. Hourly security check .....AR 190-51, para 3-3f

c. Risk Level III

1. All requirements from Levels I & II

2. Park in lighted areas .....AR 190-51, para 3-3e

2. IDS or continuous surveillance .....AR 190-51, para 3-3f

TABLE 4-2. UNARMED VEHICLES

a. Risk Level I

1. Lock vehicles & control keys .....AR 190-51, para 3-5e

2. Post off limits signs .....AR 190-51, para 3-5e

3. To the maximum extent practicable, park in motor pools protected by fence or by guards .....AR 190-51, para 3-5d

4. Remove & secure uninstalled accessories/equipment.....AR 190-51, para 3-5e

5. Prohibit master-keyed locks for multiple vehicles.....AR 190-51, para 3-5e

6. Secure items such as bolt cutters, torches, etc. that could be used to defeat vehicle security .....AR 190-51, para 3-5e

7. Check every 4 hours .....AR 190-51, para 3-5f

8. Prohibit POVs from motor pools .....AR 190-51, para 3-5f

b. Risk Level II

1. All requirements from Level I

2. Light parking areas .....AR 190-51, para 3-5e

3. Park vehicles at least 20 feet from fence .....AR 190-51, para 3-5e

4. Control entry to & exit from motor pool .....AR 190-51, para 3-5f

5. Segregate & observe certain vehicles .....AR 190-51, para 3-5f

6. Check every 2 hours .....AR 190-51, para 3-5f

7. Spot check for dispatch & operator’s permit .... FORSCOM REG 190-13

c. Risk Level III

1. All requirements from Levels I & II

2. Use ground anchors for trailers .....AR 190-51, para 3-5e

3. Place certain vehicles in secured garages .....AR 190-51, para 3-5e

4. Post as Restricted Area .....AR 190-51, para 3-5f

5. Provide written authorization for dispatch .....AR 190-51, para 3-5f

6. Check all for dispatch & operator's permit .....AR 190-51, para 3-5f

7. IDS or continuous surveillance .....AR 190-51, para 3-5f

TABLE 4-3. ARMED VEHICLES & TOWED WEAPONS SYSTEMS & COMPONENTS

a. Risk Level I 1. All requirements from Levels I & II from Table 6-2 ...FORSCOM REG 190-13 2. Close coordination with local authorities .. ..FORSCOM REG 190-13 3. Active Commo with response & police forces . . . ...FORSCOM REG 190-13 4. Active countersurveillance program .....FORSCOM REG 190-13 5. Provide 24 hour armed guard surveillance .....AR 190-11, para 5-8c *(Vehicles/towed systems with missiles / rockets in ready to fire configuration)*
b. Risk Level II 1. All requirements from Level I 2. Maintain controlled access .....FORSCOM REG 190-13 3. Hourly security checks .....FORSCOM REG 190-13 4. Post as Restricted Area .....FORSCOM REG 190-13
c. Risk Level III 1. All requirements from Levels I & II 2. Maintain continuous surveillance .....FORSCOM REG 190-13

TABLE 4-4. NIGHT VISION DEVICES & OTHER COMMO/ELECTRONIC EQUIP

a. Risk Level I

1. Provide double barrier protection to portable items...AR 190-51, para 3-6b

2. Provide barrier protection to non-portable items .....AR 190-51, para 3-6b

3. Store as far from exterior as possible .....AR 190-51, para 3-6b

4. Post "Off Limits" signs .....AR 190-51, para 3-6b

5. Control access to storage areas .....AR 190-51, para 3-6e

6. Control keys, locks and seals .....AR 190-51, App D

7. Hand receipt pilferage coded items .....AR 190-51, para 3-6f

8. Secure (by padlock) tactical communications equipment remaining on vehicles .....AR 190-51, para 3-6b

b. Risk Level II

1. All requirements from Level I

2. Store pilferage coded items separately .....AR 190-51. para 3-6c

3. Prevent POV parking within 50 ft of storage areas ....AR 190-51, para 3-6f

4. Conduct inventories .....AR 190-51, para 3-6f

5. Designate storage areas as Restricted Area . . . . . .FORSCOM REG 190-13

c. Risk Level III

1. All requirements from Levels I & II

2. Light the area .....AR 190-51, para 3-6d

3. Control landscaping .....AR 190-51, para 3-6d

4. Protect with IDS .....AR 190-51, para 3-6d

5. Review stock records .....AR 190-51, para 3-6g

6. Check every 2 hours .....AR 190-51, para 3-6g

7. Weekly visual count . . . . . .FORSCOM REG 190-13

TABLE 4-5. HEADQUARTERS (BRIGADE AND ABOVE)

a. Risk Level I

1. Access to mission critical work areas & high risk personnel controlled continuously when facility is occupied .....AR 190-51, para 3-19

2. All entrances will be secured when HQ work areas are not occupied .....AR 190-51, para 3-23

3. Parking beneath facilities will be eliminated where possible.....AR 190-51, para 3-19

4. Parking will be as far away from the facility as possible but at least thirty feet .....AR 190-51, para 3-19

5. Locate mission critical & high risk personnel in the interior of the facility, as far from the exterior as possible where feasible .....AR 190-51, para 3-19

6. Locate trash receptacles, landscaping features, and other features greater than one foot in height which potentially provide concealment for aggressors or bombs at least thirty feet from the facility .....AR 190-51, para 3-19

7. Security force responsible for HQ security will coordinate response procedures with local security/police authorities . . . . . FORSCOM Reg 190-13

8. Ensure that all critical areas; such as entrance ways, are provided adequate security lighting . .. . FORSCOM Reg 190-13

9. Maintain an active countersurveilance program, ensure that all HQ staff personnel are briefed on their responsibilities . . . . . FORSCOM Reg 190-13

b. Risk Level II

1. All requirements from level I

2. Access to the entire facility will be controlled continuously when the facility is occupied .....AR 190-51, para 3-19

3. Windows of mission critical & high risk personnel will be covered by reflective 4-mil fragment retention film & backed up by heavy drapes .....AR 190-51, para 3-19

4. Windows and doors of mission critical areas & high risk personnel work areas will be locked so that any attempt to enter through them when the facility is unoccupied will require forced entry, whose effects will be noticeable .....AR 190-51, para 3-19

5. Duress alarms will be installed in areas occupied by mission critical & high risk personnel …...AR 190-51, para 3-19

c. Risk Level III

1. All requirements from Levels I & II

2. The facility will be surrounded by a perimeter fence at a distance from the facility of at least fifty feet ...AR 190-51, para 3-19

3. The facility will be guarded and Access to the entire facility will be controlled at all times .....AR 190-51, para 3-19

4. Personnel (not assigned to the facility) who enter areas in which mission critical assets or high risk personnel are located will be searched for weapons and explosives on at least a random basis .....AR 190-51, para 3-19

TABLE 4-6. WEAPONS STORED IN UNIT ARMS ROOMS

a. Category III & IV Weapons 1. Store in approved structure .....AR 190-11, para 4-2a 2. Protect with IDS.....AR 190-11, para 4-2a 4. Conduct security checks every 24 hrs.....AR 190-11, para 4-2a 5. Light the area .....AR 190-11, para 4-2d 6. Use proper locks.....AR 190-11, para 4-2e 7. Maintain key & lock control.....AR 190-11, para 3-8 8. Control Access.....AR 190-11, para 4-19a 9. Emplace communications.....AR 190-11, para 3-6a 10. Designate as a restricted area.....AR 190-11, para 4-15
b. Category II Weapons 1. All requirements from Categories III & IV 2. Post armed guard if IDS fails.....AR 190-11, para 4-2f(1) 3. Conduct security checks every 8 hrs.....AR 190-11, para 4-2a(3)

TABLE 4-7. AA&E IN BULK STORAGE

a. Category III & IV AA&E 1. Store in approved structure.....AR 190-11, para 5-2 2. Conduct security checks every 48 hrs if unalarmed.AR 190-11, para 5-2 3 Use proper locks . . . . . AR 190-11, para 5-6a 4. Maintain key & lock control . . . . . AR 190-11, para 5-6b 5. Emplace communications. . . . . AR 190-11, para 5-7 6. Control access. . . . . .AR 190-11, para 5-9 7. Designate as a restricted area . . . . . .AR 190-11, para 5-10 8. Post signs announcing IDS, if present . . . . . AR 190-11, para 5-11 9. Conduct security checks every 72 hrs if alarmed AR 190-11, change 1
c. Category II AA&E 1. All requirements from Category III 2. Protect with IDS .....AR 190-11, para 5-2a 3. Protect with armed guards (if IDS fails) .....AR 190-11, para 5-2a(2) 4. Conduct security checks every 2 hrs.....AR 190-11, para 5-2a(2) 5. Light the area .....AR 190-11, para 5-4a
d. Category I AA&E 1. All requirements from Category II 2. Conduct security checks every hour.....AR 190-11, para 5-2a(2) 3. Implement two-person rule.....AR 190-11, para 5-9c

TABLE 4-8. UNIT MOTOR VEHICLE MOVEMENTS OF AA&E

a. Category III,IV & Un-categorized AA&E

1. Maintain under continuous control .....AR 190-11, para 7-15d

2. Use only GOV, POV not authorized .....AR 190-11, para 7-15a

3. Use the vehicle exclusively for AA&E, do not mix AA&E with other cargoes .....FORSCOM REG 190-13

4. Lock, seal or band cargo by shipper.....AR 190-11, Para 7-19

b. Category II AA&E

1. All requirements from Category III & IV

2. Place in the custody of an E-5 or above .....AR 190-11, para 7-15c

3. Category II AA&E will have armed guard surveillance when transported off post ..... AR 190-11, para 7-15c

4. Require favorable ENAC for driver and guards .....AR 190-11, para 2-11a

5. Lock and seal cargo by shipper .....AR 190-11, Para 7-19

c. Category I and CLASSIFIED AA&E

1. All requirements from Category II

2. Require custodian to have security clearance at least equal to the level of classification of AA&E being transported .....AR 55-355, para 34-2g

3. Provide an armed guard escort .....AR 190-11, para 7-15c

4. Lock and seal cargo by shipper.....AR 190-11, Para 7-19

5. Continuous audit trail by SN and/or item to consignee . . . . . AR 190-11, para 7-4a

6. Require two-person certification.....AR 190-11. para 7-4a

7. Maintain two way communications between the lead and trail vehicles .....FORSCOM REG 190-13

NOTES:

1. For commercial transportation of AA&E via motor vehicle, rail, air and sea; refer to chapter 7, AR 190-11 & AR 55-355. For transportation of AA&E during training refer to paragraph 2-5, AR 190-11.

2. Coordination must be made with local authorities concerning the requirement for armed guard surveillance of AA&E.

TABLE 4-9. RAIL MOVEMENT OF AA&E

a. Category II, III & IV AA&E

1. Ship inside locked (or equivalent system), sealed containers .....AR 190-11

2. Where possible, place containers so as to deny access to the doors of the containers .....AR 190-11

3. Require shipper to immediately notify U.S. representative when train arrives at destination ....DoD 5100.76-M

4. Hourly security checks (visual inspection of cars, locks, seals) when train is halted .....AR 190-11

5. Check and verify seals at halts lasting more than 1 hour and at final destination .....AR 190-11

b. Category I & Classified AA&E

1. All requirements from Category II, III & IV

2. Constant surveillance by armed guards .....DoD 5100.76-M

APPENDIX A
References

SECTION I
Required Publications

AR 190-11 & Change 1 dated 12 Feb 98
Physical Security of Arms, Ammunition, and Explosives

AR 190-13
The Army Physical Security Program

AR 190-16
Physical Security

AR 190-40 & FORSCOM Suppl 1 dated 1 Jun 95
Serious Incident Report

AR 190-51
Security of Unclassified Army Property (Sensitive & Nonsensitive)

AR 190-58
Personal Security

AR 380-19
Information Systems Security

AR 380-40
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 525-13
Antiterrorism

AR 710-2
Supply Policy Below the Wholesale Level

DA Pam 25-380-2
Security Standards for Controlled Cryptographic Items

DA Pam 190-51
Risk Analysis for Army Property

DA Pam 710-2-1
Using Unit Supply Systems Procedures Manual

DOD 4270.1-M
Construction Criteria

DOD 5200.2-R
Personnel Security Program

FM 19-30
Physical Security

TB 9-2300-422-20
Security of Tactical Wheeled Vehicles

TB 380-40-22
Security Standards for Controlled Cryptographic Items

TB 380-41 (series)
Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material

TM 5-853-1
Security Engineering, Designing for Security

SECTION II
Related Publications
A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 30-1
The Army Food Service Program

AR 30-18
Army Troop Issue Subsistence Activity Operating Procedures

AR 30-19
Army Commissary Store Operating Policies

AR 40-2
Army Medical Treatment Facilities; General Administration

AR 40-7
Use of Investigational Drugs in Humans and the Use of
Schedule I Controlled Drug Substances

AR 40-61
Medical Logistics Policies and Procedures

AR 40-66
Medical Record and Quality Assurance Administration

AR 58-1
Management, Acquisition and Use of Administrative Use Motor Vehicles.

AR 95-1
General Provisions and Flight Regulations.

AR 108-2
Army Training and Audiovisual Support

AR 190-27
Army Participation in National Crime Information Center (NCIC)

AR 210-6
Furniture and Household Equipment Support for Family Housing and Bachelor Housing

AR 230-1
The Nonappropriated Fund System

AR 230-65
Nonappropriated Funds: Accounting and Budgeting Procedures

AR 380-5
Department of the Army Information Security Program

AR 420-17
Real Property and Resource Management

AR 420-70
Buildings and Structures

AR 700-84
Issue and Sale of Personal Clothing

AR 703-1
Coal and Petroleum Products Supply and Management Activities

AR 708-1
Cataloging and Supply Management Data

AR 710-3
Asset and Transaction Reporting System

AR 725-50
Requisitioning, Receipt, and Issue System

AR 735-5
Policy and Procedures for Property Accountability

AR 740-26
Physical Inventory Control

AR 870-5
Military History: Responsibilities, Policies, and Procedures

AR 870-20
Historical Properties and Museums

DA Pam 738-750
The Army Maintenance Management System (TAMMS)

DOD 4525.6-M
DOD Postal Manual, Volumes I and II

TB 43-0209
Color, Marking, and Camouflage Painting of Military Vehicles, Construction Equipment, and Materials Handling Equipment

SECTION III
Referenced Forms

DA Form 1687
Notice of Delegation of Authority-Receipt for Supplies

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 2062
Hand Receipt

DA Form 2806-R
Physical Security Survey Report

DA Form 2806-1-R
Physical Security Inspection Report

DA Form 5513-R
Key Control Register & Inventory

DA Form 7281
Command Oriented AA&E Security Screening & Eval.

Standard Form 700
Security Container Information

Standard Form 701
Activity Security Checklist

Standard Form 702
Security Container Check Sheet

FORSCOM FORM 190-R
Installation Physical Security Survey

DA A Form 1687	Delegation of Authority-Receipt for Supplies
DA Form 2806-R	[see FORSCOM Form 190-R]
DA Form 2806-1-R	Physical Security Inspection
DA Form 3056	Report of Missing/ Recovered AA&E
DA Form 4261/4262-1	Physical Security Inspector Identification Card
DA Form 4604	Security Construction Statement
DA Form 4930	Alarm/Intrusion Detection Record
DA Form 5513	Key Control Register & Inventory
DA Form 7278	Risk Level Worksheet
DA Form 7281	CMD Oriented AA&E Security Screening & Evaluation

FORSCOM Form 190-R
Physical Security Survey

FORSCOM PHYSICAL SECURITY SURVEY
(FORSCOM Reg 190-13)
(See FORSCOM Reg 190-13 for instructions on completing this survey.)

PART I - ADMINISTRATIVE DATA

1. INSTALLATION	2. DATE OF SURVEY	3. DATE OF PREVIOUS SURVEY

4. OVERALL EVALUATION OF PHYSICAL SECURITY OF THE INSTALLATION. *(Attached as Enclosure 1 is a list of current installation security vulnerabilities, with a discussion of each. The discussion will contain recommendations to counter each vulnerability.)*

☐ EXCELLENT ☐ SATISFACTORY ☐ MARGINAL ☐ POOR

5. NAME(S) OF PERSONNEL CONDUCTING SURVEY

NAME	RANK	TITLE	ORGANIZATION

PART II - INSTALLATION DESCRIPTION

6. INSTALLATION MISSION STATEMENT *(Attach as enclosure if necessary)*

7. INSTALLATION COMMANDER	8. INSTALLATION PROVOST MARSHAL OR DIRECTOR OF SECURITY

9. INSTALLATION ACREAGE	10. POPULATION			
	MILITARY	FAMILY MEMBERS	CIVILIAN EMPLOYEES	TOTAL

11. NUMBER OF DESIGNATED MISSION ESSENTIAL OR VULNERABLE AREAS (MEVAs). *(Attach MEVA list as Enclosure 2, indicate date of last risk analysis for each MEVA.)*

12. NUMBER OF BUILDINGS	13. NUMBER OF TENANT ACTIVITIES *(Enclose list of tenants)*

14. TYPE INSTALLATION ACCESS

OPEN POST	CLOSED POST	NUMBER OF GATES MANNED		NUMBER OF GATES UNMANNED
		Full Time	Part Time	

15. ARE RESOURCES AVAILABLE TO PROVIDE CONTROLLED OR RESTRICTED ACCESS TO INSTALLATION AND MEVAS IAW APPROPRIATE THREATCON MEASURES? *(Barriers)*

PART III - INSTALLATION LAW ENFORCEMENT AND SECURITY FORCES

16. LIST SECURITY FORCES AVAILABLE TO SUPPORT INSTALLATION SECURITY REQUIREMENTS

TYPE	AUTHORIZED	ASSIGNED
MILITARY POLICE		
OTHER MILITARY GUARD FORCES (BMM)		
CONTRACT GUARDS		
DOD POLICE		
DOD CIVILIAN GUARDS		
OTHER		
TOTAL		

FORSCOM FORM **190-R,** 1 AUG 99

8-1/2x11

PART III - INSTALLATION LAW ENFORCEMENT AND SECURITY FORCES (CONTINUED)		
	YES	NO
17. ARE SECURITY FORCES AVAILABLE TO PROVIDE REQUIRED SECURITY/LAW ENFORCEMENT SUPPORT?		
18. ARE SECURITY FORCES TRAINED AND EQUIPPED?		
19. ARE GUARD ORDERS PUBLISHED, CURRENT AND ADEQUATE? *(For questions 16-19, if deficiences exist, provide discussion as enclosure.)*		

PART IV - PHYSICAL SECURITY PERSONNEL		
20. LIST NUMBER AND GRADES AUTHORIZED/ASSIGNED		
a. MILITARY SUPERVISOR *(Name, Rank)*	b. CIVILIAN SUPERVISOR *(Name, Grade, Title)*	
c. MILITARY INSPECTOR/PHYSICAL SECURITY INSPECTOR *(Name, Rank, MOS)*		
d. CIVILIAN PHYSICAL/SECURITY SPECIALIST(S) *(Attach list as enclosure if necessary)*		
NAME	GRADE	TITLE
21. IS STAFFING LEVEL SUFFICIENT TO SUPPORT INSPECTION REQUIREMENTS? *(If staffing not sufficient, attach discussion as enclosure.)*		

PART V - INSTALLATION PHYSICAL SECURITY PLAN
22. DATE OF CURRENT PLAN
23. DOES PLAN COVER PEACETIME, DEPLOYMENT/ MOBILIZATION CONTINGENCIES?
24. DOES PLAN CONTAIN REQUIRED ANNEXES IAW AR 190-13?
25. DOES ANTI-TERRORISM ANNEX CONTAIN PROVISIONS FOR IMPLEMENTING THE THREATCON SYSTEM?
26. ARE RESOURCES FOR IMPLEMENTING THREATCON MEASURES IDENTIFIED AND AVAILABLE?
27. DATE ANTI-TERRORISM ANNEX TO PLAN LAST EXERCISED
28. ASSESSMENT OF ADEQUACY OF PHYSICAL SECURITY PLAN AND ANNEXES *(Attach discussion as enclosure.)* ☐ ADEQUATE ☐ INADEQUATE ☐ MARGINAL

PART VI - THREAT STATEMENT
29. DATE OF INSTALLATION THREAT STATEMENT *(Attach current Threat Statement as enclosure.)*
30. DOES THREAT STATEMENT PROVIDE ADEQUATE ASSESSMENT OF LOCAL THREAT?
31. HAS THREAT STATEMENT RESULTED FROM COORDINATED EFFORT OF CID, MILITARY INTELLIGENCE, PROVOST MARSHAL, AND APPROPRIATE LOCAL LAW ENFORCEMENT AGENCIES?

PART VII - ENGINEERING/IDS
32. DOES ENGINEER/PUBLIC WORKS EMPLOY A SYSTEM THAT IDENTIFIES SECURITY RELATED WORK ORDERS?

PART VII - ENGINEERING/IDS (CONTINUED)		
33. NUMBER OF PENDING SECURITY RELATED WORK ORDERS		
34. ARE IDS INSTALLED IN ALL LOCATIONS AS REQUIRED BY REGULATION?		
35. TYPES OF IDS ARE INSTALLED *(Check all appropriate boxes)* ☐ J-SIIDS ☐ J-SIIDS WITH AMG ☐ ICIDS ☐ OTHER		
PART VIII - CRIME DATA		
36. NUMBER OF CRIME RELATED SIRs		
CURRENT CY	PREVIOUS CY	PREVIOUS 2D YEAR CY
37. INSTALLATION CRIME RATES OVER 3 YEAR PERIOD. *(Data will be graphic depiction which covers both crimes against property and against persons.)*		
38. ENCLOSURES		
INSTALLATION VULNERABILITIES AND RECOMMENDED COMPENSATORY MEASURES *(Required)*		
MEVA LISTING *(Required)*		
LIST OF RESTRICTED AREAS *(Required)*		
LIST OF TENANT ACTIVITIES *(Required)*		
DISCUSSION OF SECURITY FORCE DEFICIENCIES *(Required if significant deficiencies are found)*		
DISCUSSION OF PHYSICAL SECURITY PERSONNEL *(Required if significant deficiencies are found)*		
DISCUSSION OF SECURITY PLAN *(Required if plan is assessed as less than adequate)*		
DISCUSSION OF THREAT STATEMENT *(Required if significant deficiencies are found)*		
LIST OF WAIVERS AND EXCEPTIONS *(Required if any waiver or exception exists)*		
FACILITIES REQUIRED BY REGULATION TO HAVE IDS WITH NO IDS INSTALLED *(Include explanation for each, i.e., resources, new construction, etc.)*		
CRIME RATE CHARTS *(Required)*		
OTHER		
REMARKS		

APPENDIX B

Responsibilities

B-1. Index

This appendix consolidates physical security related responsibilities for the following:

B-2. FORSCOM Commander

a. Ensure a command physical security officer is appointed who will determine command-wide physical security needs.

b. Ensure a Physical Security Program is established.

c. Ensure resource needs for meeting physical security requirements are identified.

d. Review for content and accuracy the threat statements prepared by subordinate installations and activities.

e. Identify PSE performance requirements, and coordinate these requirements with the PSE user representative (TRADOC) and the PSEMO.

f. Ensure engineers and physical security personnel coordinate in the formulation of design criteria for new construction projects, and that physical security personnel review all planning documents, plans, and specifications at every step of the planning, design, and construction process.

g. Ensure Army forces deploying to overseas areas designate personnel to carry out physical security responsibilities to safeguard Government personnel, facilities, equipment, operations, and materiel against hostile intelligence, terrorists, other criminal, dissident, or other disruptive activity.

h. Support TRADOC in the preparation and coordination of requirements documents.

i. Provide one member (field grade officer or civilian equivalent) to the Army Physical Security Equipment Action Group (APSEAG).

B-3. FORSCOM Provost Marshal

a. Appoint a command physical security officer who will determine command-wide physical security needs.

b. Establish a Physical Security Program to plan, formulate, and coordinate physical security matters; ensuring practical, effective, and common sense measures are used.

c. Manage the Physical Security MDEP (RJC6). Identify resource needs in the planning, programming and budgeting system, and allocate necessary resources.

d. Designate the FORSCOM member (field grade officer or civilian equivalent) to the APSEAG.

e. Ensure the procedures outlined in **Chapter 3** are followed in the issue, purchase, lease, or lease renewal of PSE.

B-4. Commanders of Installations or Activities

a. Those commanders who are subject to jurisdiction or administration, or in the custody of Defense agencies or separate operating activities, will issue the necessary regulations to protect and secure personnel, places, and property under their command, per the Internal Security Act of 1950.

b. Commanding officers of designated representations, posts, camps, stations, or installations subject to DA jurisdiction or administration, or in DA custody, will also issue the necessary regulations to protect and secure personnel places and property under their command, per the Internal Security Act of 1950.

c. Appoint, in writing, an installation physical security officer who will report through channels to the commander or deputy commander on all matters related to physical security.

d. Develop an installation local security threat statement in coordination with local intelligence and law enforcement support elements, based on DA and MACOM threat statements. The physical security threat must be incorporated into the overall Force Protection threat statement.

e. Develop an installation physical security plan.

f. Ensure physical security is included as part of the OPSEC annex in all applicable orders and plans.

g. Ensure supporting military intelligence elements are given all the data relating to the organization and its activities needed to support the force protection mission.

h. Ensure the passing of threat information to all military activities on/off the installation.

i. Designate & approve restricted areas.

j. Provide physical security support to tenant activities per AR 37-49 and AR 210-10.

k. Ensure security programs provide for safeguarding of personnel, facilities, equipment, operations, and materiel during mobilization and war.

l. Designate, in writing, physical security mission essential or vulnerable areas (MEVAs) under their control.

m. Ensure all physical security MEVAs under their control requiring inspection are inspected.

n. Ensure risk analyses are performed for all facilities (new and existing) either designated or likely to be designated as physical security MEVAs.

o. Ensure engineers and physical security personnel coordinate in the formulation of design criteria for new construction projects, and that physical security personnel review all plans and specifications at every step of the planning, design, and construction process. The DA Form 1391 will be utilized for this process.

p. The commander shall consider appointing, in writing, a physical security council, to assist the commander and the security officer in discharging their security duties.

q. Coordinate physical security plans with local LEAs and supporting military intelligence (MI) and USACIDC elements.

r. Set up liaison at the local level with appropriate civilian agencies.

s. Ensure that agreements governing consolidated AA&E storage facilities and the storage of AA&E property of Federal, State, contractor agencies, and foreign government agencies contain definite assignment in writing of responsibility for the items stored.

t. Conduct unannounced inspections as often as deemed necessary by the commander concerned.

u. Ensure construction programming documents involving AA&E facilities have been coordinated with the responsible provost marshal or security officer

B-5. Commanders of Host and Tenant Activities

a. Request physical security requirements or enhancements beyond his or her means from the host commander.

b. Inform the host commander of all physical security measures in effect.

c. Defer to the authority of the installation commander on the issue of supplements to this regulation.

d. Designate their physical security MEVAs in writing, and forward this listing to the installation commander for inclusion in the installation physical security plan.

e. Forward a copy of their physical security plan to the installation commander, to be included as an annex to the installation physical security plan.

f. Host commanders will provide support to tenant activities in the areas below, unless otherwise mutually agreed in writing.

(1) Law enforcement patrols and security guards, as required to protect personnel and government assets.

(2) Installation and maintenance of Army IDS and other PSE.

(3) Monitoring and response to electronic security equipment when not within the tenant activity's capability.

(4) Minimum essential physical security support (to include installation of IDS when required) to those nonappropriated fund (NAF) income-producing tenant activities (for example, clubs and post exchanges) per NAF regulations.

(5) Inspections of tenant activities, and providing tenant commanders with copies of the inspection reports.

(6) Support tenant commanders' annual physical security training programs.

g. Commanders or directors of tenant activities (located both on and off the installation) must identify their security requirements to the host installation. They will ensure funding provisions are considered in proper budget programs.

h. Commanders or directors of activities, and units will coordinate physical security plans once a year with the installation PMO or Security Office to ensure their security procedures are current and in keeping with the command and HQDA physical security directives.

i. Include provisions in security procedures for applying physical security measures for storage areas in keeping with the host commander's assessment.

B-6. Installation PM or Physical Security Officer

a. Recommend to the commander those installation activities that should be designated as MEVAs.

b. Assess installation physical security needs by conducting physical security surveys and inspections per **Chapter 2**.

c. Recommend physical security considerations in the preparation of installation engineer construction projects, including the design phase. Ensure security considerations are included in new construction, renovation, modification efforts, or lease acquisition.

d. Serve as the installation's single point of contact (POC) for PSE for units under control of and within the AR 5-9 area of responsibility of the installation commander. Ensure coordination of equipment requirements with user, facility engineer, logistics, and communication personnel.

e. In coordination with local intelligence and law enforcement support elements, develop the installation threat statement.

f. Monitor resource management (dollars and personnel) of the installation physical security program. In coordination with the comptroller, plan and program necessary resources for physical security projects in the program budget cycle.

g. Monitor appropriate funding status of all physical security program resource requirements.

h. Coordinate physical security efforts with the organization OPSEC Officer and terrorism counteraction POC.

i. Coordinate with the installation engineer during the planning, design, and construction of all projects to identify physical security/anti-terrorism requirements, and to ensure that such requirements are incorporated into the projects at the inception of the project planning.

j. Review planning documents and construction plans and specifications for construction projects at all stages of their development.

B-7. Installation Engineer or Master Planner

a. Coordinate with the PM or physical security officer during the planning, design, and construction of all construction projects to ensure that physical security requirements are incorporated into the projects at the inception of the project planning.

b. Coordinate the review of all planning documents and construction plans and specifications at all stages of their development with the PM or physical security officer.

c. Ensure Installation planning boards include a physical security representative from the LEA, PMO or Security Office as a voting member on all actions. The representatives will ensure that provisions of this regulation are considered and made a matter of record during the planning process.

B-8. Unit Commanders and Custodians of AA&E

a. Comply with this regulation.

b. Ensure necessary measures are taken to safeguard AA&E at all times. This includes providing specific instructions on individual responsibility for AA&E during operational or field
training conditions, care and maintenance, competitive marksmanship meet, and storage on, or when mounted on, vehicles and aircraft.

c. Ensure timely submission of serious incident reports (SIR) per AR 190-40, paragraph 4-9.

d. Report all losses (actual or suspected) or recoveries within 2 hours of initial detection to the proper law enforcement agencies.

e. Conduct prompt investigation of losses after a decision of the USACIDC that criminal acts were not involved.

f. Fix responsibility when negligence is determined and take proper corrective action to prevent further loss.

g. Publicize AA&E security and loss prevention through command information and unit training programs.

h. Plan, program, budget, and allocate resources for the implementation of required policies outlined in this regulation.

i. Ensure that AA&E storage facilities are checked, inventoried, and inspected as required by this regulation.

B-9. Key Custodians

a. Ensure they have written appointment orders specifying their responsibility to issue and receive keys and maintain accountability for office, unit, or activity keys.

b. Ensure individuals, who clearly understand local key control procedures, are designated to issue, receive, and account for keys in their absence.

c. Maintain a key control register at all times to ensure continuous accountability for keys of locks used to secure Government property.

APPENDIX C
Checklists

C-1. Purpose
This appendix provides checklists that may be used to quickly check for compliance with physical security requirements.

C-2. General
The checklists are not intended to be used in lieu of the pertinent regulations. The checklists are only guides and quick references. The checklists may not cover all security requirements for a particular subject area. Checklists are designed to contain the same material as found in the Security Management System (SMS). The SMS is a primary tool of FORSCOM physical security inspectors. Physical security inspections will be based on SMS, not on the checklists provided in this regulation.

C-3. Index of Checklists

TABLE A
STAFF ASSISTANCE VISIT CHECK LIST

Yes	No	NA	
			1. Are trained physical security personnel assigned to the Physical Security Office (ASI H3/GS-080)? AR 190-13, Para 3-3
			2. Have MEVAs, which the Physical Security Office is responsible for inspecting, been identified? AR 190-13, Par 2-4
			3. Are inspections being conducted every 18 months for AA&E related MEVAs and every 24 months for all other MEVAs? AR 190-13, Para 2-11
			4. Are AA&E storage facilities re-inspected within 6 months if they fail the initial inspection? AR 190-11, Para 2-6a(4)
			5. Is there a Physical Security Officer who supervises the physical security program? AR 190-13, Para 1-25
			6. Is there a functioning Joint Action Work Group or Physical Security Council, which meets regularly to discuss physical security related issues? AR 190-13, Para 1-23c
			7. Are physical security personnel aware of the relationship between physical security and force protection? AR 190-13, Para 2-5
			8. Does the physical security office have at least the following references on hand: AR 190-11 AR 190-13 AR 190-16 AR 190-51 AR 525-13 FC 190-13 DA PAM 190-51 FM 19-30
			9. Does the Physical Security Office have a copy of all active waivers and exceptions for facilities within their area of operation? AR 190-11, Para 2-4i and AR 190-51, Para 1-6
			10. Does the Physical Security Office maintain a database of intrusion detection systems (IDS) by type/location/status? FC 190-13. Para 3-16

NOTE: This checklist provides for a review of the overall status of a physical security program.

TABLE B
UNIT ARMS ROOM CHECK LIST

A. CONSTRUCTION

Yes	No	NA	
			1. Does the Unit have a DA Form 4604-R (Security Construction Statement) not more than 5 years old, in the arms room indicating the highest category of weapons/ammunition authorized for storage? AR 190-11, Para 2-2d
			2. If deficiencies are listed on the DA Form 4604-R are compensatory measures taken until the deficiencies are corrected? AR 190-11, Para 2-4
			3. Has a request for an exception been submitted for uncorrectable deficiencies noted on a physical security inspection or is one on file in the arms room? AR 190-11, Para 2-4
			4. Is the arms room door provided with exterior security lighting? AR 190-11, Para 4-2d
			5. Are switches for exterior lights installed so that they are not accessible to unauthorized individuals? AR 190-11, Para 4-2d(4)
			6. Are exterior security lights covered with mesh screen or vandal resistant lenses that will prevent their being broken? AR 190-11, Para 4-2d(5)
			7. Does the door allowing access to arms room containing Category I and II arms meet the established criteria? AR 190-11, App G
			8. Are arms room doors, other than the main entrance, secured from the inside with locking bars, dead bolts or with approved secondary padlocks (American Series 200 or 5200)? AR 190-11, Para 4-2e(1)
			9. Are the door hinges of the fixed pin security hinge type or equivalent? Are exposed hinge pins pinned, spot welded, or otherwise secured to prevent removal? AR 190-11, Para 4-2a, App G, para G-1d(3)
			10. Are bars or steel mesh, which protects windows and openings, embedded into the structure of the building, or welded to a steel frame that is securely attached to the wall with the fastening inaccessible from the exterior of the arms storage facility? AR 190-11, App G, Para G-1e
			11. Are High Security padlock(s) (Sergeant & Greenleaf (S&G) Model 831B, NSN 5340-01-188-1560; Hi-Shear Model LK 1200, NSN 5340-00-799-8248; or model S&G 833C NSN 5340-01-217-5068) used in conjunction with High Security hasp to secure the arms room door? AR 190-11, Para 4-2e(1) **Note:** On a double door system, the high security lock and hasp will be on the most secure door. The most secure door will normally be the one meeting the specifications in item 9 above. Secondary padlocks with hardened steel shackle (American Series 200 or 5200) may be used to secure the other door.
			12. Are weapons stored within the arms room secured in standard issue racks or locally fabricated arms racks or metal containers that are certified by the local engineers (DEH) and is the certificate filed in the arms room? AR 190-11, Para 4-2c(3)
			13. Are all weapons racks and containers secured in a way to prevent removal of AA&E and locked with approved secondary padlock (American Series 200 or 5200)? AR 190-11, Para 4-2c(2)&(3)

			14. Are weapons racks and ammunition containers, weighing less than 500 lbs., fastened to the

			walls or floors, or chained together in groups totaling more than 500 lbs.? Are the chains secured with approved secondary padlock (American Series 200 or 5200) and is the chains heavy duty, hardened steel, galvanized of at least 5/16 inch thickness? AR 190-11, Para 4-2c(2)
			15. Are restricted Area signs posted near the entrance on the exterior wall of the arms room, at eye level? AR 190-11, Para 4-4 and AR 190-13, para 6-4
			16. Are signs posted on the exterior of each interior wall that contains an entrance to the arms storage room, vault or building announcing the presence of IDS? AR 190-11, Para 4-5

B. ARMS ROOM KEY CONTROL

Yes	No	NA	
			1. Are primary and alternate Key and Lock custodians appointed in writing to ensure the proper custody and handling of arms room keys and locks? AR 190-11, para 3-8c
			2. Does the unit have a current roster of personnel authorized to receive the Arms Room keys, signed by the designated unit official and protected from public view? AR 190-11, Para 3-8a
			3. Are inventories of keys and locks conducted semiannually and are the results documented and retained for one year? The inventories can be documented on DA Form 5513-R. AR 190-11, Para 3-8e
			4. Does the key and lock custodian maintain a "RECORD" (DA Form 5513-R, AUG 93, Key Control Register) identifying all keys/locks and combinations to locks used to secure arms room racks, containers, security chains and all replacement or reserve keys and locks? AR 190-11, Para 3-8c
			5. Is a DA Form 5513-R's used to ensure positive control of keys, and establish responsibility for the custody of stored AA&E and retained for 90 days when completed? AR 190-11, Para 3-8a
			6. Have padlocks and/or keys which do not have a serial number given one? AR 190-11, Para 3-8e
			7. Are keys providing access to Category I or II AA&E which are not in use or not attended stored in a Class 5 GSA security container or equivalent? AR 190-11, Para 3-8b(2) and DoD 5100.76-M, Chapter 3, Para H1b
			8. Are keys providing access to Category III or IV AA&E which are not in use or not attended stored in a container of at least 20 gauge steel, or equivalent strength and equipped with approved secondary padlock (American Series 200 or 5200) or a GSA-approved built-in 3-position changeable combination lock? AR 190-11, Para 3-8b(2)
			9. In the event of lost, misplaced, or stolen keys, has an investigation been initiated immediately? Replacement or reserve locks, cores and keys will be secured immediately to preclude access by unauthorized individuals. AR 190-11, Para 3-8b(3)
			10. Are padlocks not in use secured to the staple or hasp when the area or container is open to preclude theft, loss or substitution of the lock? AR 190-11, Para 3-8d
			11. Are master key systems or multiple key systems used? This is prohibited. AR 190-11, Para 3-8b(3)
			12. Are keys to arms room storage buildings, rooms, racks, IDS, or containers removed from the Installation? AR 190-11, Para 3-8a
			13. When the responsibility for Arms Room Keys is transferred between two authorized individuals, do both parties conduct a physical count of all arms and ammunition stored in the arms room? DA Pam 710-2-1, Para 9-11a(1)
			14. Is this count recorded on DA Form 2062, and maintained on file until the next serial number inventory is conducted. DA Pam 710-2-1, Para 9-11a(2)

C. INTRUSION DETECTION SYSTEM (IDS)

Yes	No	NA	

			1. Is the arms room manned, under constant surveillance (by individuals) or have an active IDS and checked by a security patrol (SDO/SDNCO/Guard) at least once each 8 hours? AR 190-11, Para 4-2a(3)
			2. In the event the IDS fails, is an armed guard posted 24 hours each day to: maintain constant unobstructed observance of the storage structure(s), prevent any unauthorized access to the storage structure(s), and make known any unauthorized access to the storage structure(s)? AR 190-11, Para 4-2f(1)
			3. Is the IDS Control Unit door key (maintenance key) kept separate from other operational IDS keys and access permitted only to authorized maintenance personnel? The key custodian may sign out the keys to the approved DEH maintenance personnel, however they must be inventoried during the semiannual inventory. AR 190-11, Para 3-8a
			4. Do personnel closing the protected area (Arms Room), ensure that the Control Unit is changed from "ACCESS" to "SECURE" before departing the arms room area?
			5. Are procedures in effect at the Monitoring station to verify the identity of personnel before opening and closing a facility protected by IDS? (Observation)
			6. Is a response force identified and capable of responding to an alarm within 15 minutes or less? AR 190-11, Para 3-6a
			7. Is a DA Form 5513-R AUG 93, (Key Control Register) maintained for issue and receipt of IDS keys? AR 190-11,Para 3-8
			8. Do arms room personnel have a list of personnel authorized to perform maintenance, repair and testing of IDS?

D. ACCOUNTABILITY OF PRIVATELY OWNED FIREARMS (POF), AMMUNITION AND OTHER WEAPONS

Yes	No	NA	
			1. Are POF, ammunition and weapons stored in unit arms rooms tagged with the name, grade, SSN and DEROS of the owner, make, caliber, serial number of the weapon, registration number and expiration date of the registration?
			2. Are POF, Ammunition and other weapons secured in the arms room, stored separate from military AA&E and protected by the same security measures, including inventory and accountability, that are required for government Arms and Ammunition? AR 190-11, Para 4-5a
			3. Do personnel desiring to use their POF obtain written permission from their commander and sign the weapon out using the same sign out/sign in procedures as those required for government weapons AR 190-11, Para 4-5b (4)
			4. Are POF ever carried on field training exercises by anyone?
			5. Are prohibited Items stored in the arms room? AR 190-11, para 4-18

E. SECURITY SCREENING PROGRAM

Yes	No	NA	
			1. Has the command conducted a security screening program for all personnel who are assigned to duties which involve responsibility for the control, accountability, and shipment of AA&E?. AR 190-11, Para 2-11a
			2. Are security screening checks recorded on DA Form 7281-R and retained in unit files until the individual departs, or is relived of his or her AA&E oriented duties? AR 190-11, Para 2-11
			3. Have government employees (civilian or military) operating a vehicle or providing security to a vehicle transporting Category I, II or classified AA&E been the subject of a favorable NAC, ENTNAC or Foreign National Screening? AR 190-11, Para 2-11a(1)
			4. Have personnel authorized unaccompanied access to Category I and II AA&E been the subject of security screening program? The security screening must include: Personal

			interviews by the individual's commander, medical files check, personnel records check, and Provost Marshal files check? AR 190-11, Para 2-11c
			5. Are security screening checks updated every three years? AR 190-11, Para 2-11e

F. USE AND CONTROL OF PROTECTIVE SEALS

Yes	No	NA	
			1. Is a primary and alternate Seal custodian appointed in writing and maintain a hard cover log book which reflects: Seal serial number; Date issued; Name of recipient; Using office, unit, activity or activity; Identification of items to which applied, Date and Time applied; Location of item. AR 190-51, **Appendix D**, Para D-10c
			2. Are all seals not issued for actual use secured in a locked metal container with controlled access by the primary and alternate custodian and a recorded monthly inventory conducted? AR 190-51**, Appendix D**, Para D-10b(6)
			3. Have procedures been established for checking seals and identifying actions to be taken upon finding a broken seal? AR 190-51, **Appendix D**, Para D-10e
			4. Are used seals defaced to prevent unauthorized reuse and properly disposed of? AR 190-51, **Appendix D**, Para D-10f

G. MISCELLANEOUS

Yes	No	NA	
			1. Has a written SOP been established for the activity, approved through command channels and maintained on file? AR 190-11, Para 1-12a
			2. If the facility is a consolidated arms room, have procedures been established to fix responsibility for access, issue, receipt, and physical accountability for all items in writing by Letter of Agreement identifying the unit which has responsibility for overall security of the facility? AR 190-11, Para 4-4
			3. If Ammunition is stored in the arms room is it consistent with the operational requirements, authorized in writing by the unit commander and inventoried by lot number during the monthly serial number inventories? AR 190-11, Para 5-8c(a) and DA Pam 710-2-1, Para 9-11b(3)
			4. Is the ammunition authorized for storage in arms room, stored in separate containers from weapons and secured in banded crates, or metal containers equivalent to standard issue metal wall lockers? AR 190-11, para 5-8c(2)
			5. Are monthly serial number weapon inventories being conducted by the responsible officer or an NCO, warrant officer, commissioned officer, or DOD civilian appointed by the responsible officer and not by the same person in consecutive months? AR 710-2, Para 2-12 and DA Pam 710-2-1, Para 9-11b
			6. For USAR, are serial number inventories conducted quarterly, and physical counts during the other two months of the quarter?
			7. During arms room serial number/sensitive items inventories, is loose ammunition that is not banded and in sealed containers, counted and annotated on the inventory sheet reflecting total rounds on hand by type? Ammunition in banded or sealed containers must be counted by containers and inspected to ensure bands and seals are in tact. DA Pam 710-2-1, Para 9-11b(3)
			8. Are the monthly arms room inventory records maintained for a minimum of 2 years or 4 years if discrepancies are found? AR 190-11, Para 6-2b(2)(b)1
			9. Are tools such as hammers, bolt cutters and chisels, which could be used to assist unauthorized persons in gaining access to arms storage facilities, readily accessible to intruders? Tools of this type should be removed from the vicinity of the arms room and locked in a container. AR 190-11, Para 4-18a
			10. Is the most recent Physical Security inspection report maintained on file in the unit? AR 190-13

			11. Have deficiencies (findings), noted on inspection reports, been corrected and action taken reported back to the Provost Marshal Office by "Reply by Endorsement (RBI)"? AR 190-11
			12. Are Category II AA&E storage facilities checked (not exceed 8 hours) by a security patrol on an irregular basis after duty hours? These checks should be recorded on SF 702, and maintained on file for 90 days. AR 190-11, Para 4-2f(2)(a)
			13. Has the commander provide written approval for storage of high value items such as night vision devices, compasses, field glasses and etc., in the arms room? AR 190-11, Para 4-18
			14. Has a "two person rule" been established for access to Category I A&E storage facilities? AR 190-11, Para 5-9c
			15. Are inert and expended launcher tubes, inert mines, and inert rocket launcher training devices, and practice rockets, secured as category IV AA&E? AR 190-11, Para 5-2c(3)
			16. Has the Unit Armorer signed for all the property in the arms room? AR 710-2, Para 2-10

TABLE C
UNIT MOTOR POOL & GOVT PROP SECURITY CHECK LIST

Yes	No	NA	
			1. Has a risk analysis been conducted on the facility to determine the level of physical security measures and procedures required? AR 190-51, **Chapter 2**.
			2. When Army vehicles are not in use, are they parked in a motor pool protected by a perimeter fence or dedicated guards? AR 190-51, Para 3-5d
			3. Is the fence around the motor pool, constructed according to guidance found in Field Manual (FM) 19-30, Army Corps of Engineers Drawing No. 40-16-08, Type FE-5 or NATO standard design? AR 190-51, Para 3-1d
			4, Is the perimeter fence in adequate state of repair? AR 190-51, Para 3-1d and FM 19-30, **Chapter 5**
			5. Is the perimeter fence clear zone adequately maintained to prevent unobserved detection of an intruder? AR 190-51, Para 3-1d, FM 19-30, **Chapter 5**, Para 5-12
			6. Is the motor pool checked at least once every 4 hours, for tampering, sabotage, loss or damage? AR 190-51, Para 3-5f(1)(a)
			7. Do commercial vehicles have activate manufacturer installed door and ignition-locking device(s)? AR 190-51, Para 3-5e(1)(a)
			8. Are tactical vehicles and other Army vehicles secured with a chain and padlock so as to immobilize the steering wheel to prevent the vehicle from being driven? Hood, spare tires and fuel tank should also be secured if the local environment warrants. AR 190-51, Para 3-5e(1)(b)&(c)
			9. Do material handling equipment (fork lift, etc) have their steering mechanisms immobilized or transmission lever locked in the neutral position? AR 190-51, Para 3-5e(1)(d)
			10. Are inoperable, unserviceable vehicles protected from cannibalization? AR 190-51, Para 3-5e(2)(d)
			11. Are accessible and easily removable components, vulnerable to theft because of value or utility, removed from vehicles and secured separately? Components will be secured: In storage structures, locked totally enclosed armed vehicles or truck van, locked equipment box or similar container secured directly to the vehicle by a locally fabricated method. AR 190-51, Para 3-5e(3)
			12. Is a primary and alternate Key and Lock custodian appointed in writing to ensure the proper custody and handling of all keys and locks? AR 190-51, Para 3-5e(5) (See Table D, Key & Lock Control)
			13. Are Privately Owned Vehicles (POV) prohibited from motor pools? The installation commanders may authorize POV storage in motor pools during unit deployment exercises. AR 190-51, Para 3-5f(1)(c)
			14. Are items which can be used to defeat security measures, such as bolt cutters, hacksaws, axes and steel bars or rods, secured when not in use? AR 190-51, Para 3-5e(6)
			15. Do Level II motor pools have both entry and exit controlled? Control may be by guards or locked gates. AR 190-51, Para 3-5f(2)(b)
			16. Are vehicles in level II or III, motor pools parked at least 20 feet form the perimeter of the parking area or as far from the perimeter as possible? AR 190-51, Para 3-5e(7)(c)
			17. Are vehicles particularly vulnerable to theft, misappropriation, or damage in level II motor pools segregated to where guards or unit personnel can readily see them? AR 190-51, Para 3-5f(2)(c)
			18. Are level II motor pools checked at least once every 2 hours, for tampering, sabotage, loss or damage? AR 190-51, Para 3-5f(2)(d)
			19. Are level III motor pools posted as a restricted area? AR 190-51, Para 3-5f(3)(b)
			20. Are level III motor pools under continuous surveillance by guards? ESS may be used for continuous surveillance. AR 190-51, Para 3-5f(3)(e)
			21. Are vehicles with missiles/rockets in ready to fire configuration provided with constant armed guard protection? AR 190-11, Para 5-8c(4)

			22. Has the unit commander or their designated representative provided written authorization before vehicles in level III motor pools are dispatched? AR 190-51, Para 3-5f(3)(c)
			23. Are drivers checked for possession of a valid dispatch and operator's permit before they depart a level III motor pool? AR 190-51, Para 3-5f(3)(d)
			24. Do POL tank trucks that contain fuel and not under surveillance by the operator or guard have, locked hatch covers, locked manifold access doors, manifold valve secured with a seal if manifold access door cannot be locked? **Note**: Use specified non-sparking brass locks for safety. AR 190-51, Para 3-14a
			25. Is packaged POL secured in an adequate storage area? AR 190-51, Para 3-13b(1)(c)
			26. Are POL credit cards, identification plates and aviation fuel plates controlled? AR 190-51, Para 3-13c(1)(c)
			27. Are POL pumps, not activated by a credit card type device, locked and electrical power turned off when not under constant surveillance? AR 190-51, Para 3-13b(1)(b)
			28. Are serviceable used and new repair parts secured in adequate single storage area, accessible only to maintenance or supply personnel, AR 190-51, Para 3-11f(3) and 3-12
			29. Are non-portable repair parts secured inside a building or protected by a perimeter barrier? AR 190-51, Para 3-11c(2)
			30. Are tool sets/kits secured with a padlock and along with other tools stored in a secure location when not in use? AR 190-51, Para 3-22b & c

TABLE D
UNIT KEY AND LOCK CONTROL CHECK LIST

Yes	No	NA	
			1. Is a primary and alternate Key and Lock custodian appointed in writing to ensure the proper custody and handling of all keys and locks? AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-2a
			2. Does the key and lock custodian maintain a control register (DA Form 5513-R, AUG 93, may be used) to ensure continuous accountability for keys of locks used to secure Government property?. AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-2c & D-3
			3. Are keys providing access to government property which are not in use or not attended stored in a container (not containing classified material) or depository made of at least 26-gauge steel, equipped with a tumbler-type locking device and permanently affixed to a wall or equivalent? AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-4a
			4. Is there an access roster maintained in the key depository listing those authorized to issue and receive keys? AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-3
			5. Is the key to the depository secured when not in use? AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-5c
			6. Are master key systems or multiple key systems used? This is prohibited except as noted elsewhere in AR 190-51. AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-5
			7. Have padlocks and/or keys which do not have a serial number been given one? AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-6e
			8. Are inventories of keys and locks conducted semiannually and are the results documented and retained until the next inventory is conducted? The inventories can be documented on DA Form 5513-R. AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-3 & D-6b
			9. In the event of lost, misplaced, or stolen keys, has an inquiry been initiated immediately? Replacement or reserve locks, cores and keys will be secured immediately to preclude access by unauthorized individuals. AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-6c
			10. Are padlocks and keys not in use secured in a locked container that does not contain classified material and access controlled to the container? AR 190-51, Para 1-4e(6) and **Appendix D**, Para D-5c
			11. Are keys for Arms Rooms kept separate from other keys? AR 190-11, Para 3-8a

APPENDIX D
Physical Security Plans

D-1. Physical Security Planning Considerations

a. Physical security requirements will be integrated into all plans (peacetime, contingency operations, mobilization and war) to ensure conservation of physical security resources and effective protection of personnel, facilities, and equipment within Army responsibility.

b. Physical security planning will be tied to the defense readiness condition system and the terrorist threat conditions outlined in AR 525-13.

c. Physical security plans should be designed to protect against:

(1) Hostile intelligence gathering operations.
(2) Paramilitary forces.
(3) Terrorists.
(4) Traditional criminal elements.
(5) Protest groups.
(6) Disaffected persons.
(7) Saboteurs.

D-2. Coordination

a. In developing physical security plans, coordination and close liaison should be effected between the military commander and:

(1) Adjacent installations or units.
(2) Federal agencies.
(3) State and local agencies.

b. To the extent permissible, such interaction should allow for an exchange of intelligence, information on security measures being employed, contingency plans, and any other information to enhance local security.

c. On an installation, the host activity shall assume responsibility for coordinating physical security efforts of all tenants, regardless of the DOD components represented, as outlined in the support agreements and the host activity security plan.

d. The purpose of such coordination is protection in depth. Authority, jurisdiction, and responsibility must be set forth in a manner that ensures protection and avoids duplication of effort.

D-3. Contingency Plans

Contingency plans must be included in any physical security planning. During periods of natural disaster, emergency, or periods of increased threat from terrorist or criminal elements; it will be necessary to increase security for sensitive assets, such as key facilities; arms, ammunition and explosives; high value, pilferable items; etc. Contingency plans should include provisions for increasing the physical security measures and procedures based on the local commander's assessment of the situation. These provisions should be designed for early detection of an attempted intrusion, theft, or interruption of normal security conditions.

D-4. Threat Assessment

a. The first step in security planning is to evaluate the threat. The physical security threat is a subset of the overall Force Protection threat assessment. Installations will develop a local physical security threat statement, this statement will identify local threats, and make full use of the investigative resources available in the geographic area to anticipate criminal and intelligence activities that threaten the physical security of Army property and personnel. At a minimum, liaison shall be established with the following agencies:

(1) Local FBI field office.
(2) State & Local law enforcement agencies.
(3) Military Intelligence agencies.
(4) Military investigative agencies.
(5) Local Bureau of ATF field office.

b. Installation physical security threat statements will be disseminated to all subordinate and tenant activities. Dissemination may be as part of the overall Force Protection threat statement. The physical security threat statement will be the basis for the installation physical security plan as outlined below.

D-5. Physical Security Plan Format

The physical security plan within FM 19-30 may be used as a guide in developing the installation physical security plan. Annexes to the plan may be separated for operational purposes and located in other installation documents as required; however, the location of the annexes will be listed in the physical security plan. The physical security plan, including all annexes, will be exercised at least once every two years in order to evaluate its effectiveness. As a minimum, the plan will include:

a. The physical security portion of the Force Protection Threat Statement.
b. Terrorism counteraction planning.
c. Procedures for dealing with bomb threats.
e. Contingency plans to deal with natural disasters.
f. Civil disturbance plan.
g. Resource plan.
h. Communications plan.
i. List of designated restricted areas.
j. List of installation MEVAs.

APPENDIX E
Unit Arms Room Security Guide

E-1. General. This guide is intended to aid unit armorers in meeting the regulatory requirements for arms room security and accountability. Below are 10 standards to be met by all unit arms rooms and the basic requirements contained within each standard. This guide is not intended to serve as a substitute for AR 190-11, it merely provides a quick reference for personnel involved in operating unit level arms rooms. Refer to AR 190-11 for detailed security requirements for security of AA&E.

E-2. Construction Criteria. AA&E will be stored only in facilities which meet construction standards specified within AR 190-11.

a. Qualified engineer personnel will verify the structural composition of the arms room (e.g. walls, ceiling, doors, floor) on DA Form 4604-R, Security Construction Statement.

b. The DA Form 4604-R will clearly indicate the highest Category of AA&E the facility meets and the date of applicable regulations.

c. DA Form 4604-R will be posted in the arms room.

d. DA Form 4604-R must be reviewed during inspections and be revalidated every 5 years by the engineers.

E-3. Access Control Measures. Commanders will ensure that access to AA&E is controlled at all times.

a. The arms room must be designated and posted as a restricted area.

b. Commanders will limit access to the unit arms room to the least practical number, with particular attention to the control of unaccompanied access.

c. The name and duty position of persons authorized unaccompanied access to the arms room will be on a list signed by the unit commander and posted inside the facility.

d. Armorers will be armed at the discretion of the unit commander.

E-4. Background Checks. Commanders will determine the reliability and trustworthiness of personnel before they are assigned duties involving control of AA&E.

a. Minimum screening by the Commander includes:

(1) Personal interview.

(2) Check medical record (mental disorders).

(3) Check personnel record (Courts Martial, ART 15)

(4) Criminal records check (MP records, local civilian agencies - if permitted)

b. Security screening must be repeated at least every three years.

E-5. Intrusion Detection Systems (IDS). The arms room, if not continuously manned or under constant surveillance, must be protected by IDS. The IDS must consist of at least two types of sensors, one of which is a volumetric sensor. (**See Chapter 3**)

a. If the arms room is protected by IDS, signs displaying the fact that IDS is present must be posted**. (See Chapter 3**)

b. During non-duty hours, arms rooms storing Category I & II weapons protected by IDS must be checked on irregular 8 hour intervals. Category III & IV storage facilities must be checked on irregular 24 hour intervals.

c. Quarterly operational checks of the IDS must be conducted and recorded. (**See Chapter 3**)

d. Civilian contractors involved in the maintenance, design, and operation of IDS must have at least a confidential clearance.

E-6. Key Control. Only DA approved keys and locks will be used to secure AA&E and they will be maintained under continuous control.

a. Only DA approved locks and locking devices (including hasps and chains) will be used.

b. Keys and combinations associated with the arms room will be under positive control at all times. Keys will be signed out only to authorized personnel and will be signed out on a key control register (DA Form 5513). Completed registers will be retained on file for a minimum of 90 days.

c. Keys to arms room doors, racks, containers and keys required for the maintenance and repair of IDS (including keys to the control unit door and monitor cabinet), will be maintained separately from other keys, and accessible only to those individuals whose duties require access to them.

d. A roster indicating individuals authorized access to arms room keys will be maintained, the roster will be protected from public view. The roster, when not in use, will be kept in a controlled, locked container.

e. When not in use, or under custodial control (SDO/SDNCO), keys to CAT I or II AA&E will be stored in approved Class V, GSA security containers. Keys to CAT III or IV AA&E will be stored in containers of at least 20-gauge steel or material of equivalent strength. Keys will **not** be stored in the same containers with classified materials. NOTE: A separate drawer of a classified container, which contains no classified materials, is acceptable for key storage.

f. A key and lock custodian will be appointed in writing. The custodian is responsible for procurement and accountability of keys and locks.

g. To preclude theft, loss or substitution, arms room padlocks will be locked to the staple or hasp when the area or container they secure is open.

h. A key and lock inventory containing a record of keys and locks, their serial numbers, locations and numbers of keys per lock will be maintained in the key depository.

i. When custody of arms room keys is transferred, they must be accounted for by serial number unless they have been placed in a sealed container. Evidence indicating that the seal has been tampered with will require a serial number inventory of all AA&E within the storage area which the keys secure. Any change of custody must be recorded in writing.

E-7. Lighting. The area around arms rooms will be adequately lighted to ensure unauthorized activity within close proximity to the arms room can be observed.

a. Switches for exterior lights will be installed so that they are not accessible to unauthorized personnel.

b. There must be security lighting at the entrance and the issue window of the arms room.

c. Interior and exterior lighting will be provided for all arms rooms, lighting will be sufficient to enable the observation of acts such as forced entry or removal of AA&E from the facility.

d. Exterior lights will be protected by screens or other covers that prevent lights from being broken by thrown objects.

E-8. Storage Criteria. All storage of AA&E will be IAW approved DA security criteria.

a. All arms racks or containers will be locked with low security U.S. Army approved padlocks, series 200/5200.

b. Privately owned weapons/ammunition may be authorized by the commander for storage in the unit arms room, however, they must be secured in locked containers which are separate from those storing government AA&E.

c. Unless a facility is manned 24 hours per day, racks and other containers weighing less than 500 pounds will be either fastened to the structure or to each other in groups weighing at least 500 pounds.

d. Bolts used to secure racks will be spot welded, brazed, or peened to prevent easy removal.

e. Chains used to secure racks and containers will be heavy duty hardened galvanized steel, welded, straight links, of at least 5/16-inch thickness, or of equivalent resistance to the force required to cut or break a secondary padlock.

f. Hinged locking bars for racks will have the hinge pins welded or otherwise secured to prevent easy removal.

g. All racks will be constructed so that weapons can not be removed from the rack by disassembling the weapon and/or rack.

h. Locally fabricated racks may be used if they provide protection equivalent to standard Army racks. The local engineer must certify, in writing, that fabricated racks are constructed according to technical data package (TDP) sketches and assembly instructions. The certification must be maintained on file in the location where such racks are used. TDP may be requested from Commander, U.S. Army Armament, Munitions and Chemical C Command, ATTN: AMSMC-MAG-SS, Rock Island, IL 61299-6000.

E-9. Inspections. Arms rooms will undergo periodic inspection to ensure compliance with security procedures.

a. A physical security inspection is required before and immediately after initial occupancy of an arms room, when a significant change is made to the facility's structure, and after any forced entry (or attempted forced entry) of the facility.

b. A Physical Security Inspection of the arms room, by a credentialed physical security inspector, will be conducted at least every 18 months.

c. In the event a facility receives an inadequate rating, a re-inspection will be conducted within 6 months.

d. Scheduled announced or unannounced Physical Security Inspections may be conducted at the discretion of the Installation Physical Security Officer.

E-10. Inventories. AA&E will be inventoried monthly to ensure accountability and chain of custody.

a. When custody of the arms room is transferred between authorized persons, they will conduct a physical count of all weapons and ammunition stored therein. Results will be recorded on DA Form 2062.

b. Arms room keys and locks will be inventoried, by serial number, semiannually. Keys and locks without serial numbers will be given a serial number. Inventory records will be maintained on file for a minimum of one year.

c. A monthly weapons and sensitive items inventory, (USAR quarterly serial number inventories and monthly physical counts) by serial number, will be conducted by an individual designated by the commander. The individual conducting the inventory will meet the grade requirements IAW AR 710-2. Individuals will not perform successive monthly inventories. Written records of inventories will be maintained, these records will be kept on file for 2 years or 4 years if discrepancies are noted.

E-11. Issue/Turn-In Procedures. To maintain continuous control and ensure chain of custody, AA&E will be issued and turned in only IAW approved, documented procedures. Positive control of all AA&E will be maintained at all times. The AA&E will be receipted for when taken from the arms room. All issue and turn-in requirements are set forth in DA Pam 710-2-1, para 5-5.

GLOSSARY

SECTION I
Abbreviations

AA&E
Arms, Ammunition, and Explosives

ARNG
Army National Guard

ASL
Authorized Stockage List

CCI
Controlled Cryptographic Items

CCTV
Closed-Circuit Television

COMSEC
Communications Security

CONEX
Container Express

CONUS
Continental United States

CONUSA
Armies in the Continental United States

CUCV
Commercial Utility and Cargo Vehicle

DA
Department of the Army

DEH
Director of Engineering and Housing

DOD
Department of Defense

DOL
Director of Logistics

DPW
Director of Public Works

FM
field manual

GBL
Government Bill of Lading

GSA
General Services Administration

IDS
Intrusion Detection System

MACOM
Major Army Command

MEDCEN
U.S. Army Medical Center

MEDDAC
Medical Department Activity

MEVA
Mission Essential/Vulnerable Area

MHE
Material Handling Equipment

MUSARC
Major U.S. Army Reserve Command

NATO
North Atlantic Treaty Organization

NCIC
National Crime Information Center

NCO
Noncommissioned Officer

NFESC
Naval Facilities Engineering Services Center

NGR
National Guard regulation

NSN
National Stock Number

OCIE
Organizational Clothing and Individual Equipment

OPSEC
Operations Security

POL
Petroleum, Oil, and Lubricants

RDT&E
Research, Development, Test, and Evaluation

SF
Standard Form

SOP
Standing Operating Procedure

SSSC
Self-Service Supply Center

TASC
Training and Audiovisual Support Center

TB
technical bulletin

TISA
Troop Issue Subsistence Activity

TM
Technical Manual

TMDE
Test, Measurement, And Diagnostic Equipment

TNT
Trinitrotoluene

USACIDC
United States Army Criminal Investigation Command

USAR
U.S. Army Reserve

USS
United States Standard

SECTION II
Terms

Access
(when pertaining to a restricted area or CCI) Personnel movement within a restricted area that allows the chance for visual observation of, or physical proximity to, either classified or protected material. The ability and opportunity to obtain detailed knowledge of CCI through uncontrolled physical possession. External viewing or escorted proximity to CCI does not constitute access.

Ammunition
A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame for use in connection with defense or offense including demolition. Excluded from this definition are devices charged with chemical agents defined in JCS Pub. 1 and nuclear or biological material. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or having a unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition and caliber .22 ammunition are excluded.

Antiterrorism measures
Physical protective measures and operational measures used to reduce the vulnerability of individuals and property to terrorist acts.

Arms
A weapon included in **Appendix A** of AR 190-11 that will or is designed to expel a projectile or flame by the action of an explosive, and the frame or receiver of any such weapon.

Asset
Any resource requiring protection.

Aviation facility

A Department of the Army activity or area collocated with facilities for the takeoff and landing of aircraft. The facility has the mission of command and control of administrative, operational, training, and/or logistical support of Army aviation.

Bulk storage
Storage in a facility above the using/dispensing level specifically applicable to logistics warehouse and depot stocks. Applies to activities using controlled medical substances and items (such as pharmacies, wards, or clinics) only when a separate facility (building or room) is used to store quantities that exceed normal operating stocks.

Commercial-Type Vehicle
A vehicle designed to meet civilian requirements, and used without major modifications, for routine purposes in connection with the transportation of supplies, personnel, or equipment.

Container Express
A reusable container for shipment of troop support cargo, quasimilitary cargo, household goods, and personal baggage.

Constant surveillance
Continuous, unobstructed observance of items or an area to prevent unauthorized access. Continuous surveillance may be maintained by dedicated guards, other on-duty personnel, or intrusion detection systems and enhanced by closed-circuit television.

Controlled Area
See restricted area.

Controlled Cryptographic Item
A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but is controlled.

Controlled Medical Substance
A drug or other substance, or its immediate precursor, listed in current schedules of 21 USC 812 in medical facilities for the purpose of treatment, therapy, or research. Categories listed in this section are narcotics, amphetamines, barbiturates, and hallucinogens.

Cryptographic Component
The embodiment of a cryptographic logic in either hardware or firmware form, such as a modular assembly, a printed circuit board, a microcircuit, or any combination of these.

Cryptographic Equipment
Any equipment employing a cryptographic logic.

Cryptographic Logic
A deterministic logic by which information may be converted to an unintelligible form and reconverted to an intelligible form. Logic may take the form of engineering drawings, schematics, hardware, or firmware circuitry.

Dedicated Guards
Individuals charged with performing the primary task of safeguarding designated facilities, material, and personnel within a defined area during a tour of duty. A dedicated guard may perform this function as a static post. He or she remains within or on the perimeter of a protected area and maintains continuous surveillance over that which is being protected during the tour of duty.

Disaffected Persons

Persons (military, DA civilians, family members, others) who are discontented or resentful and may exhibit this by damaging, destroying or stealing government property, or causing harm to other personnel.

Double Barrier Protection
Two physical barriers of protection provided to defeat or deter illegal entry. Examples of double barrier protection are**:**

a. A locked or guarded separate building or an enclosed van, trailer, or armored vehicle protected by a perimeter fence.

b. A locked steel cage located in a secure storage structure.

c. A locked, built-in container (bins, drawer, cabinet) or free-standing locked container located in a secure storage structure.

Double-Locked Container
A steel container of not less than 26 gauge which is secured by an approved locking device and which encases an inner container that also is equipped with an approved locking device. Cabinet, medicine, combination with narcotic locker, NSN 6530-00-702-9240, or equivalent, meets requirements for a double-locked container.

Electronic Security System (ESS)
Collect term to describe a variety of security equipment such as alarms, CCTV, card readers, etc that are electronic in nature.

Emergency Vehicle
A vehicle designated by the commander to respond to emergency situations and provide life-saving and property-saving services. Normally, the vehicle has special equipment and markings. Ambulances and fire fighting and military or security police vehicles are examples.

Enclosed Vehicle or Equipment
A conveyance that is fully enclosed with permanent sides and permanent top, with installed doors that can be locked and sealed.

Entry Control (when pertaining to a restricted area)
Security actions, procedures, equipment, and techniques employed within restricted areas to ensure that persons who are present in the areas at any time have authority and official reason for being there.

Escorted personnel (when pertaining to a restricted area)
Those persons authorized access to a restricted area who are escorted at all times by a designated person.

Escorts and Couriers
Military members, U.S. civilian employees, or DOD contractor employees responsible for the continuous surveillance and control over movements of classified material. Individuals designated as escorts and couriers must possess a Government-issued security clearance at least equal to that of the material being transported.

Exception
An approved permanent exclusion from specific requirements of this regulation. Exceptions will be based on a case-by-case determination and involve unique circumstances which make conformance to security standards impossible or highly impractical. An approved permanent deviation from the provisions of this regulation. There are two types of exceptions:

a. Compensatory Measures Exception. A deviation in which the required standards are not being met, but the DOD component (MACOM) concerned determines it is appropriate, because of physical factors and operational requirements. Compensatory measures are normally required.

b. Equivalent Protection Exception. A deviation in which nonstandard conditions exist, but the totality of protection afforded is equivalent to or better than that provided under standard criteria.

Explosives
Any chemical compound, mixture, or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual land mines, demolition charges, blocks of explosives (dynamite,

trinitrotoluene (TNT), C-4, and other high explosives), and other explosives consisting of 10 pounds or more; for example, gunpowder or nitroguanidine.

Force Protection
Security program developed to protect soldiers, family members, civilian employees, facilities and equipment, in all locations and situations. This is accomplished through the planned integration of combating terrorism, physical security, information operations, high-risk personnel security, and law enforcement operations. All supported by foreign intelligence, counterintelligence and other security programs.

Handling
Controlled physical possession without access.

High Risk Personnel
Personnel who, by their grade, assignment, symbolic value, location, or specific threat, are more likely to be attractive or accessible terrorist or other criminal targets.

Industrial and Utility Equipment
Equipment used in the manufacture or in support of the manufacture of goods and equipment used to support the operation of utilities such as power and water distribution and treatment.

Installations
Such real properties as reserve centers, depots, arsenals, ammunition plants (both contractor- and Government-operated), hospitals, terminals, and other special mission facilities, as well as those used primarily by troops.

Internal Controls (when pertaining to a restricted area)
Security actions, procedures, and techniques employed within restricted areas to ensure persons who are present in these areas at any time have authority and official reason.

Intrusion Detection System
The combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into the area protected by the system and reporting directly to an alarm monitoring station. The IDS will be an approved DOD standardized system, such as the Joint Service Interior Intrusion Detection System or MACOM approved commercial equipment.

Key and Lock Control System
A system of identifying both locks and their locations and personnel in possession of keys and/or combinations.

Keying
The process of establishing a sequence of random binary digits used to initially set up and periodically change permutations in cryptographic equipment for purposes of encrypting or decrypting electronic signals, for controlling transmission security processes, or for producing other keys.

Limited Area
See restricted area.

Locked Container
A container or room of substantial construction secured with an approved locking device. For pharmacy operating stocks, lockable automated counting systems meet requirements for a locked container.

Medically Sensitive Items
Standard and nonstandard medical items designated by medical commanders to be sufficiently sensitive to warrant a stringent degree of physical security and accountability in storage. Included within this definition are all items subject to misappropriation and/or misuse such as needles and syringes.

Mission-Critical Personnel
Personnel who are essential to the operation of an organization or function.

Mission essential or Vulnerable Areas
Facilities or activities within the installation that, by virtue of their function, are evaluated by the commander as vital to the successful accomplishment of the installation's State National Guard or MUSARC mission. This includes areas nonessential to the installation's operational mission but which, by nature of the activity, are considered vulnerable to theft, trespass, damage, or other criminal activity.

Motor Pool
A group of motor vehicles used as needed by different organizations or individuals and parked in a common location when not in use. On an Army installation, a nontenant Army activity with 10 or less assigned commercial-type vehicles but no local organizational maintenance support does not have a motor pool, under this regulation, even through the vehicles are parked together.

Motor vehicle
A self-propelled, boosted, or towed conveyance used to transport a burden on land. This includes all Army wheeled and track vehicles, trailers, and semitrailers, but not railroad locomotives and rolling stock.

Note C Controlled Medical Items
Sets, kits, and outfits containing one or more component Note Q or Note R items.

Note Q Controlled Medical Items
All standard drug items identified as Note Q in the Federal
Supply Catalog, Nonstandard Drug Enforcement Administration (DEA) Schedule III, IV, V Controlled Substances.

Note R Controlled Medical Items
All items identified as Note R in the Federal Supply Catalog. Nonstandard DEA Schedule II Controlled Substances.

Paramilitary Forces
Organized body formed on a military pattern, such as a militia group.

Perimeter Fence
Fences for the security of unclassified, nonsensitive items that meet the requirements of U.S. Army Corps of Engineers Drawing No. 40-16-08, Type FE-5. The minimum height will be 6 feet. Use of NATO Standard Design Fencing is also authorized.

Physical Protective Measures
Physical security measures used to counter risk factors that usually do not change over a period of time such as mission impact, cost, volume, and criticality of resources and vulnerabilities. The measures are usually permanent and involve expenditure of funds.

Physical Security
That part of security concerned with measures taken to deter, detect and defend against the spectrum of criminal threats to personnel, property, and facilities. The threats include terrorists, saboteurs, vandals, paramilitary forces, disaffected persons, etc.

Physical Security Procedures
Include, but are not limited to, the application of physical measures to reduce vulnerability to the threat; integration of physical security into contingency, mobilization, and wartime plans; the testing of physical security procedures and measures during the exercise of these plans; the interface of installation OPSEC, crime prevention and physical security programs to protect against the traditional criminal; training of guards at sensitive or other storage sites in tactical defense against and response to attempted penetrations; and creating physical security awareness.

Physical Security Measures
Physical systems, devices, personnel, animals, and procedures employed to protect security interests from possible threats and include, but are not limited to, security guards; military working dogs; lights and physical barriers; explosives and bomb detection equipment; protective vests and similar equipment; badging systems; electronic entry control systems and access control devices; security containers; locking devices; electronic intrusion detection systems; standardized command, control, and display subsystems; radio frequency data links used for physical security; security lighting; delay devices; and assessment and/or surveillance systems to include closed-circuit television. Depending on the circumstances of the particular situation, security specialists may have an interest in other items of equipment such as armored sedans.

Physical Security Equipment
A generic term for any item, device, or system that is used primarily to protect Government property, including nuclear, chemical, and other munitions, personnel, and installations, and to safeguard national security information and material, including the destruction of such information and material both by routine means and by emergency destruct measures.

a. Interior physical security equipment. Physical security equipment used internal to a structure to make that structure a secure area. Within DOD, DA is the proponent for those functions associated with development of interior physical security systems.

b. Exterior physical security equipment. Physical security equipment used external to a structure to make the structure a secure area. Within DOD, the Department of the Air Force is the proponent for those functions associated with the development of external physical security systems; however, the Army will develop lights and barriers.

c. Intrusion detection system. See previous definition.

Physical Security Inspection
A formal, recorded assessment of procedures and physical measures implemented by a unit or activity to protect its assets. Normally conducted for an individual MEVA.

Physical Security Plan
A comprehensive written plan providing proper and economical use of personnel, land, and equipment to prevent or minimize loss or damage from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.

Physical Security Program
The interrelationship of various components that complement each other to produce a comprehensive approach to security matters. These components include, as a minimum, the physical security plan; physical security inspections and surveys; and a continuing assessment of the installation's physical security posture.

Physical Security Survey
A formal, recorded, review of the overall security posture of an installation (multiple MEVA).

Pilferage-Coded Items
Items with a code indicating that the material has a ready resale value or civilian application and, therefore, is especially subject to theft.

Portable
Capable of being carried in the hand or on the person. As a general rule, a single item weighing less than 100 pounds (45.34 kilograms) is considered portable.

Restricted Area
Any area to which entry is subject to special restrictions or control for security reasons or to safeguard property or material. This does not include those designated areas over which aircraft flight is restricted. Restricted areas may

be of different types. The type depends on the nature and varying degree of importance, from a security standpoint, of the security interest or other matter contained therein.

a. Exclusion area. A restricted area containing--

(1) A security interest or other matter of such nature that access to the area constitutes, for all practical purposes, access to such security interests or matter; or--

(2) A security interest or other matter of such vital importance that proximity resulting from access to the area is treated equal to (1) above.

b. Limited area. A restricted area containing a security interest or other matter, in which uncontrolled movement will permit access to such security interest or matter; access within limited areas may be prevented by escort and other internal restrictions and controls.

c. Controlled area. That portion of a restricted area usually near or surrounding an exclusion or limited area. Entry to the controlled area is restricted to authorized personnel. However, movement of authorized personnel within this area is not necessarily controlled. Mere entry to the area does not provide access to the security interest or other matter within the exclusion or limited area. The controlled area is provided for administrative control, safety, or as a buffer zone for security in depth for the exclusion or limited area. The proper commander establishes the degree of control of movement.

Risk
The degree or likelihood of loss of an asset. Factors that determine risk are the value of the asset to its user in terms of mission criticality, replaceability, and relative value and the likelihood of aggressor activity in terms of the attractiveness of the asset to the aggressor, the history of or potential for aggressor activity, and the vulnerability of the asset.

Risk Analysis
A process used to decide the level of security warranted for protection of resources. It involves examining the value of and threat to specific assets.

Risk Level
An indication of the degree of risk associated with an asset based on risk analysis. Risk levels may be Levels I, II, or III, which correspond to low, medium, and high.

Safe
A GSA Class 5 Map and Plans Security Container, Class 6 Security Filing Cabinet or refrigerator or freezer, secured with an approved locking device and weighing 500 pounds or more, or secured to the structure to prevent removal.

Schedule I Drug
Any drug or substance by whatever official name (common, usual, or brand name) listed by the DEA in Title 21 of the Code of Federal Regulations, chapter II, Section 308.11, intended for clinical or non-clinical use. A list of Schedule I drugs and substances is contained in AR 40-7, **Appendix A**.

Seal
A device to show whether the integrity of a container has been compromised. Seals are numbered serially, are tamperproof, and shall be safeguarded while in storage. The serial number of seal shall be shown on Government Bills of Lading (GBL). A cable seal lock provides both a seal and locking device.

Sealed Containers
Wooden boxes, crates, metal containers, and fiber containers sealed in a way to show when the containers are tampered with after sealing. The method of sealing depends of the type of construction of the containers. Sealing may be by metal banding, nailing, airtight sealing, or wax dripping (for fiber containers). In key control, a sealed container is also a locked key container or a sealed envelope containing the key or combination to the key container.

Security Lighting
Lighting used to permit surveillance by security forces or by supervisory personnel. Also applies to lighting used to deter criminal activity.

Security Procedural Measures
Operational procedures that provide a measure of security for a particular asset. Examples would include the requirement for inventory, appointment of personnel to perform specific duties which enhance security, etc.

Sensitive Conventional Arms, Ammunition, and Explosives
See categorization of such items in **Appendix A**, AR 190-11.

Sensitive Items
Material requiring a high degree of protection to prevent unauthorized acquisition. This includes arms, ammunition, explosives, drugs, precious metals, or other substances determined by the Administrator, Drug Enforcement Administration to be designated Schedule Symbol II, III, IV, or V under the Controlled Substance Act of 1970.

Storage
Any area where AA&E are kept. Storage does not include items in process of manufacture, in use, or being transported to a place of storage or use.

Tactical Vehicle
A vehicle with military characteristics designed primarily for use by forces in the field in direct connection with, or support of, combat or tactical operations, or the training of troops for such operations.

Waiver
Temporary relief from specific standards imposed by this regulation. Waivers are normally granted only for the time required to accomplish actions that will bring the activity into conformance with the standards required. Compensatory measures are required until the standard is met.